



REVISTA D'INTERNET, DRET I POLÍTICA  
REVISTA DE INTERNET, DERECHO Y POLÍTICA

IDP Número 27 (Septiembre, 2018)

DOSIER

# «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»



Universitat  
Oberta  
de Catalunya

<http://idp.uoc.edu>

ISSN 1699-8154

# IDP Número 27 (Septiembre, 2018)

## DOSIER «IMPLICACIONES JURÍDICAS DE LOS USOS Y COMENTARIOS EFECTUADOS A TRAVÉS DE LAS REDES»

### Presentación

*Albert González Jiménez* ..... 3-4

### La libertad de expresión en las redes sociales

*Laura Díez Bueso* ..... 5-16

### Los delitos de odio en las redes sociales

*Josep M. Tamarit Sumalla* ..... 17-29

### Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)

*Carmen Tomás-Valiente Lanuza* ..... 30-41

### El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento

*Beatriz López Pesquera* ..... 42-51

### Juicios paralelos en las redes sociales y proceso penal

*Vicente C. Guzmán Fluja* ..... 52-66

### Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre

*Teresa Armenta Deu* ..... 67-78

**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## PRESENTACIÓN

# Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes

Albert González Jiménez

Estudios de Derecho y Ciencia Política (UOC)

Fecha de publicación: septiembre de 2018

En el presente volumen de carácter monográfico se han recogido diversos trabajos que tratan aspectos relacionados con las implicaciones jurídicas de los usos y comentarios efectuados en las redes sociales.

La evolución de la sociedad de la información y el uso de las redes sociales han dejado al descubierto la existencia de nuevas plataformas idóneas para la comisión de delitos, así como numerosos comportamientos cuyas implicaciones jurídicas son innegables.

La apariencia de anonimato que enmascara el uso de las redes sociales es una de las principales razones por las cuales han proliferado los delitos cometidos a través de las mismas; por otra parte, se hacen incontables los mensajes de dudoso gusto y legalidad. Basta echar un vistazo a Twitter para poder ver la existencia de numerosos comentarios que o bien constituyen manifestaciones directas, o indirectas, de odio, o bien afectan a la intimidad de aquellos sobre los que se vierten, a su honor o a la propia dignidad; por no hablar de otras plataformas que, a través del intercambio, o la compraventa de objetos y servicios, han sido escogidas para la comisión de delitos patrimoniales como la estafa o la receptación.

Ahora bien, aunque todos estos comportamientos -delictivos o no, pero con claras implicaciones jurídicas- están sucediendo ante nuestros propios ojos, las dificultades probatorias que entrañan su aportación al procedimiento judicial que pueda instarse con ocasión de los mismos distan mucho de la simple captura de pantalla del comentario, del ataque al honor o del negocio fallido ofertado que quiere demostrarse. Por lo tanto, cómo deben ser aportados al procedimiento y el peso que tienen en la vida cotidiana son asuntos que merecen una observación individualizada.

El hecho de estudiar conjunta o paralelamente la libertad de expresión y los delitos de odio en las redes sociales, junto con los delitos contra la intimidad –mientras analizamos los juicios paralelos que se están llevando a cabo en dichas redes–, así como su repercusión en el proceso penal, aunado a la incertidumbre existente en la regulación legal y la valoración de las fuentes de prueba digital, pasando por los delitos de contenido patrimonial en esas mismas redes sociales, es la oportunidad que nos brinda, precisamente, este monográfico.

### Cita recomendada

GONZÁLEZ JIMÉNEZ, Albert (2018). «Presentación». En: «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 3-4. UOC [Fecha de consulta: dd/mm/aa]  
<http://dx.doi.org/10.7238/idp.v0i27.3167>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre el autor

Albert González Jiménez  
 agonzalezjim@uoc.edu

Estudios de Derecho y Ciencia Política (UOC)

Doctor en Derecho con la calificación de excelente *cum laude*. Licenciado en Derecho y en Criminología. Profesor de Derecho procesal penal, Derecho penal y Criminología en la UOC, UPF y UNED en los grados de Derecho, Criminología y en el máster de Acceso a la Abogacía. Abogado especialista en Derecho penal y Proceso penal con más de 20 años de ejercicio, tres de ellos como abogado fiscal sustituto. Ponente y director en numerosas jornadas en el ámbito de los procesos penales. ORCID: 0000-0001-7785-0810

UOC  
 Av. Carl Friedrich Gauss, 5  
 08860 Castelldefels



**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## ARTÍCULO

# La libertad de expresión en las redes sociales

Laura Díez Bueso  
 Universitat de Barcelona

Fecha de presentación: abril de 2018  
 Fecha de aceptación: junio de 2018  
 Fecha de publicación: septiembre de 2018

## Resumen

La irrupción de la comunicación a través de redes sociales obliga a los juristas a ofrecer una respuesta razonada a la siguiente cuestión: ¿los límites de la libertad de expresión son distintos si el mismo mensaje se vierte en la red o si se difunde a través de los canales tradicionales de comunicación?

Para ofrecer una respuesta desde el Derecho, resulta preciso concretar cuáles son aquellos elementos que diferencian ambos tipos de comunicación y que resultan relevantes para el análisis. A nuestro juicio, estos elementos son los siguientes: la posición del receptor del mensaje, que ha dejado de ser pasiva para convertirse en un usuario activo; la posición de relativa igualdad del emisor del mensaje; la gran cantidad y variedad de contenidos en la red; y el aumento de la capacidad de interrelación comunicativa.

Identificados estos elementos, deben confrontarse con los parámetros clásicos que el Tribunal Europeo de Derechos Humanos ha utilizado para marcar los límites de la libertad de expresión. Los parámetros que se consideran relevantes para el análisis son: la materia sobre la que versa el mensaje; la intención del emisor; quién emite el mensaje; a través de qué canal; y el ámbito geográfico donde se difunde.

De esta confrontación puede concluirse que, con la jurisprudencia de la Corte Europea en la mano, no existen argumentos jurídicos que justifiquen una distinción en los límites de la libertad de expresión en función de si el mensaje se difunde o no a través de redes sociales.

## Palabras clave

libertad de expresión, internet, redes sociales, Tribunal Europeo de Derechos Humanos

## Tema

libertad de expresión y redes sociales

## Freedom of expression on social networks

### Abstract

*The emergence of communication via social networks has forced lawyers to offer a reasoned response to the following question: are the limits of freedom of expression different if the message is transmitted via social networks rather than traditional communication channels?*

*To offer a legal response to this question, it is necessary to specify the elements that are different between both types of communication which are relevant for the analysis. We consider these elements to be the following: the position of the person receiving the message (who was previously passive but is now an active user), the position of relative equality of the person sending the message, the huge quantity and variety of content on the Internet and the increased capacity for communicative interaction.*

*Having identified these elements, they should be measured against the classic parameters used by the European Court of Human Rights to establish the limits of freedom of expression. The parameters considered relevant for the analysis are: the subject of the message, the intention of the sending party, the person who sends the message, the channel it is sent through and the geographical environment in which it is sent.*

*By measuring the elements against these parameters, and taking the jurisprudence of the European Court into account, it can be concluded that there are no legal arguments justifying a distinction in the limits of freedom of expression based on whether or not a message is sent via social networks.*

### Keywords

*freedom of expression, Internet, social networks, European Court of Human Rights*

### Topic

*freedom of expression and social networks*

## 1. Nuevas formas de comunicación y libertad de expresión

La irrupción de internet ha provocado una profunda transformación a muchos niveles, también en la comprensión de los derechos fundamentales. Esta circunstancia se hace palmaria en el caso de la libertad de expresión que, como consecuencia de este nuevo canal de comunicación, está atravesando un claro proceso de reformulación.

Este proceso tiene múltiples aristas, que van desde un replanteamiento del concepto de autoría a una transformación del modo en que los medios de comunicación desarrollan su actividad,<sup>1</sup> pasando por la brecha digital.<sup>2</sup>

La importancia de todos estos cambios resulta vital, pues están directamente conectados con nuestro sistema democrático. La respuesta final que ofrezcamos a cada uno de estos temas redundará en una mayor o peor salud democrática. En definitiva, la inevitable repercusión de las

1. Boix y López García han analizado ampliamente cómo la red ha potenciado la dilución de la noción de autoría y cómo la tecnología digital ha transformado la actividad de los medios de comunicación (2005, pág. 96-99 y pág. 81-96, respectivamente).
2. Un estudio sobre el marco general de la fractura digital en España puede encontrarse en Robles, Molina y De Marco (2012, pág. 795-810).

redes sociales en la libertad de expresión implica una reconstrucción de esta libertad donde nos jugamos el futuro del pluralismo en nuestras sociedades.

En este marco, el tema de los límites de la libertad de expresión respecto de otros derechos resulta clave. Los cambios sociales, económicos y culturales han incidido sistemáticamente en la determinación de estos límites. Recientemente, por ejemplo, el terrorismo internacional ha provocado cortapisas a la libertad de expresión que no se hubieran admitido tan solo unos años atrás.<sup>3</sup> Y, también en la actualidad, se plantea una nueva y relevante pregunta sobre los límites de la libertad de expresión conectada con recientes cambios en los usos comunicativos de nuestra sociedad: ¿los límites varían cuando los mensajes se difunden a través de redes sociales? En otras palabras, ¿un mensaje tiene los mismos límites si se envía por Twitter o si se publica en la prensa escrita? En suma, ¿es mayor o menor la libertad de expresión cuando el mensaje se transmite a través de una red social?

¿Qué respuesta debe ofrecerse desde un punto de vista jurídico? Como es sabido, el Derecho debe brindar respuestas distintas a supuestos de hecho distintos. Por ello, debe comenzarse por discernir cuáles son aquellos elementos que diferencian la comunicación a través de redes sociales respecto del resto de comunicaciones tradicionales.<sup>4</sup> Concretamente, deben identificarse aquellos elementos que pueden tener una repercusión directa en la configuración de los límites de la libertad de expresión.<sup>5</sup> A nuestro juicio, son los siguientes.

En primer lugar, la posición del receptor del mensaje ha dejado de ser pasiva para devenir un usuario activo, pues cuando lo estime pertinente puede convertirse en emisor y participar en foros de discusión, publicar documentos o enviar mensajes. Este nuevo modelo de emisor de mensajes plantea, en ocasiones, el problema de la identificación del autor de la información y de su fiabilidad.

En segundo lugar, la red coloca al emisor en una posición de igualdad, pues ofrece al ciudadano la posibilidad de llegar potencialmente a tantas personas como las corporaciones con más recursos económicos y tecnológicos. Aunque esta igualdad es muchas veces más aparente que real, dado que la red original ha ido dejando paso a una red copada por grandes empresas que la emplean de manera cada vez más masiva como instrumento de negocio.

En tercer lugar, en la red coexisten contenidos de muy diverso tipo, que van de iniciativas empresariales que movilizan grandes presupuestos a espacios creados por ciudadanos sin más pretensión que poner sus opiniones a disposición de la sociedad. En este contexto, se ha defendido una supuesta menor seriedad de los contenidos vertidos en las redes sociales, dada la pluralidad de emisores y su menor profesionalidad respecto de los medios de comunicación tradicionales.

Finalmente, la red ha propiciado un aumento de la capacidad de los ciudadanos de interrelacionarse de forma mucho más ágil y masiva. No obstante, también ha propiciado una mayor exposición pública y la indelebilidad de los mensajes difundidos, que se almacenan y quedan no solo en la memoria colectiva sino también en la digital.

3. Un caso paradigmático fue *Holder v. Humanitarian Law Project*, sustanciado en 2010 ante el Tribunal Supremo estadounidense. En este asunto se condenó a una asociación que asesoraba al Partido de los Trabajadores del Kurdistán (PKK) para que resolviera sus disputas con el Gobierno turco a través de medios legales y pacíficos. Sobre los detalles de este caso desde la perspectiva de la libertad de expresión puede consultarse Cole (2012, pág. 147-177).
4. Estos elementos se han extraído de la lectura de diversos académicos especialistas en la materia, que han sistematizado las características de la comunicación en la red; de entre ellos, se ha tomado como especial referencia a Boix (2002, pág. 146 y 162; y 2016, pág. 60) y a Carrillo (2013, pág. 14). Puede encontrarse una tipología completa de los distintos medios de comunicación e interacción social disponibles en internet en López García (2005, pág. 94-195).
5. No se van a abordar todos los elementos que distinguen la comunicación en la red respecto de la comunicación tradicional, pues no todos tienen una incidencia directa en los límites de la libertad de expresión. Así, por ejemplo, se excluyen características tan básicas como su compleja configuración técnica, que complica el control de sus contenidos y que ha hecho que autores como Muñoz Machado sean partidarios de tender hacia la autorregulación de los propios actores (2000).

## 2. Aplicación de los límites clásicos de la libertad de expresión a la comunicación en red

Hasta aquí se ha dejado constancia de la trascendencia del momento actual respecto de la determinación de los límites de la libertad de expresión. La irrupción de las redes sociales impone la necesidad de plantear el interrogante de si los límites tradicionales siguen siendo válidos o si conviene una reformulación. En este contexto, se ha advertido de la relevancia de la respuesta que ofrezcamos a este interrogante para el futuro de nuestra democracia.

Para dar respuesta a esta cuestión, se ha considerado pertinente comenzar por identificar cuáles son los elementos que distinguen la comunicación en red respecto de la comunicación tradicional. En este sentido, han sido cuatro los elementos considerados relevantes: la posición del receptor del mensaje, que puede en cualquier momento interactuar respecto del mismo y convertirse en emisor (a veces anónimo o poco fiable); la posición de relativa igualdad del emisor del mensaje; la gran cantidad y variedad de contenidos en la red; el aumento de la capacidad de interrelación comunicativa, que a su vez provoca una mayor exposición al conocimiento público y la indelebilidad de los mensajes.

Llegados a este punto, deben repasarse cuáles son los límites clásicos de la libertad de expresión para confrontarlos con estos elementos distintivos de la comunicación en red.<sup>6</sup> En otras palabras, debe analizarse si estos límites clásicos pueden aplicarse *mutatis mutandi* a un modo de comunicación distinto al tradicional cual es la comunicación a través de redes sociales.

Como es por todos conocido, el Tribunal Europeo de Derechos Humanos ha insistido una y otra vez en el peculiar estatus de la libertad de expresión, reconocida en el artículo 10.1 del Convenio Europeo de Derechos Humanos de 1950. Resulta ya habitual aludir a la Sentencia *Handyside v. Reino Unido* (1976) cuando afirma que esta libertad constituye uno de los fundamentos esenciales de la sociedad democrática, una de las condiciones básicas para su progreso y para el desarrollo de las personas.

No obstante, también es sabido que el artículo 10.2 del Convenio abre la puerta a ciertas limitaciones al prever que el ejercicio de esta libertad «podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial».

A partir de este precepto, la jurisprudencia europea ha dictaminado que, cuando un Estado limita la difusión de un mensaje, la Corte debe verificar que esta restricción cumple con los siguientes requisitos: debe hallarse prevista normativamente; perseguir una o más de las finalidades establecidas en el artículo 10.2 del Convenio; y ser una limitación necesaria en una sociedad democrática.

A partir de aquí, el TEDH analiza una serie de parámetros para decidir si la limitación a la libertad de expresión tiene cabida en el Convenio: la materia sobre la que versa el mensaje; la intención del emisor; quién emite el mensaje; a través de qué canal; y el ámbito geográfico donde se difunde. Estos parámetros no han sido todavía aplicados a la comunicación a través de redes sociales, de manera que debe interpretarse si los mismos son válidos para este tipo de comunicación, si deben aplicarse de otro modo o, incluso, si conviene buscar otros parámetros.

### 2.1. ¿Sobre qué materia versa el mensaje?

Un parámetro fundamental para determinar el límite a la libertad de expresión es la materia sobre la que versa el mensaje: en tanto que en asuntos políticos el límite se restringe, en asuntos religiosos las restricciones pueden ser superiores.

En el primer ámbito material y en coherencia con la concepción de la libertad de expresión como fundamento del sistema democrático, la Corte es clara cuando afirma que tanto en las cuestiones políticas como en asuntos

6. La literatura que analiza la jurisprudencia del TEDH relativa a los límites de la libertad de expresión es muy extensa. Un trabajo completo y sistemático puede encontrarse en Weber (2009).



de interés público existe un pequeño margen para las restricciones del artículo 10.2 (Erbakan v. Turquía, 2006). El concepto de interés público empleado por el TEDH es muy amplio: abarca desde la discusión política sobre el nacionalsocialismo en Austria en el caso Schwabe v. Austria (1992) hasta la necesidad de un servicio nocturno de urgencias para animales domésticos en el caso Barthold v. Alemania (1986).<sup>7</sup> Por otro lado, la protección que la Corte otorga a la libertad de expresión varía en función del grado de interés de lo difundido y el margen de limitación es superior cuanto más alejado está el tema de los asuntos políticos; así, en el caso Cyprus v. Turquía (2001), el TEDH advierte de que la necesidad de cualquier restricción debe establecerse de forma convincente, particularmente cuando la naturaleza del debate es política más que cuando es comercial.<sup>8</sup>

En el polo opuesto a los mensajes de carácter político, el margen para las limitaciones se amplía enormemente cuando conciernen a temas religiosos. El argumento utilizado por el TEDH para permitir una mayor limitación en asuntos religiosos radica en que, a su juicio, no existe un concepto claro y común de religión en los estados miembros del Consejo de Europa. Una de las formulaciones de este razonamiento se encuentra en la Sentencia Leyla Sahin v. Turquía (2005), donde se explica que la ausencia de una concepción uniforme sobre el significado de la religión en la sociedad y el hecho de que la expresión pública de una creencia difiera según el momento y el contexto hacen que la normativa relacionada con las ofensas a la religión deba dejarse hasta cierto punto en manos de los estados.

Como se ha expuesto, una de las características de la comunicación a través de redes sociales es el gran abanico de temas que coexisten en la red. La facilidad de emitir mensajes provoca que surjan contenidos relativos a las materias más variadas y opiniones muy diversas sobre las mismas. En este contexto, parece que no existe ningún obstáculo para aplicar a las redes sociales el parámetro de la materia sobre la que versa el mensaje utilizado por el TEDH. Es más, teniendo en cuenta la multiplicidad de

contenidos que conviven en la red, este parámetro resulta de especial utilidad en el momento de valorar los límites de la libertad de expresión en las redes sociales. Así, los mensajes que más cerca se sitúen de los asuntos políticos merecerán una protección superior y cuanto más se alejen de este ámbito su garantía se difuminará, hasta llegar al ámbito de los asuntos religiosos donde, según la Corte, las restricciones pueden ser superiores.

## 2.2. ¿Qué intención tiene el emisor?

El TEDH utiliza la intención del emisor como otro parámetro básico para determinar los límites a la libertad de expresión.<sup>9</sup> La pregunta concreta que la Corte se formula es si el emisor intentó difundir ideas, por ejemplo, racistas, o si por el contrario trataba de informar sobre asuntos de interés general. Por ejemplo, en el caso Lehideux e Isorni (1998), los demandantes no fueron considerados culpables de apología del delito por la Corte, pues se apreció que no intentaban negar o revisar lo que en su propia publicación calificaban de «persecuciones y atrocidades del nazismo». En el caso Jersild v. Dinamarca (1994), el TEDH consideró inapropiada la condena por complicidad del periodista demandante, quien había entrevistado a una serie de miembros del grupo The Greenjackets, que habían realizado afirmaciones abiertamente racistas en un programa de televisión; además del gran interés público de la materia, la Corte no consideró que objetivamente el periodista hubiera tenido el propósito de propagar esas ideas. No obstante, no puede dejar de reseñarse que esta jurisprudencia convive con sentencias como la Sürek v. Turquía (1999), donde el demandante y propietario de una revista semanal fue condenado por publicar dos cartas al director que criticaban vehementemente las acciones militares en el sudeste de Turquía; en ambos casos, la Corte sostuvo que el demandante proveyó a sus autores de un canal para incitar a la violencia y el odio y, además, como propietario tenía el poder de modelar la dirección editorial de la revista.

Respecto de la intención del emisor del mensaje, no parece que haya inconveniente en aplicar este parámetro a

- 
7. Una detallada explicación sobre los temas que el TEDH ha considerado de interés general puede verse en Díez Bueso (2002, pág. 221-222).
  8. A esta conclusión llega Díez Bueso (2002, pág. 236). Una aproximación a este planteamiento y similares conclusiones pueden leerse en Lezertúa (1993).
  9. Existe cierta coincidencia doctrinal en considerar que la intención del emisor es un elemento fundamental para el TEDH. En este sentido, véase Weber (2009, pág. 33-46) y Tulkens (2012).

la comunicación en red. Al igual que sucede en las comunicaciones más tradicionales, existen ciertos elementos que permiten determinar si la intención del emisor ha sido transmitir una opinión, criticarla o defenderla, aunque no siempre sea sencilla esta valoración y exista margen para la subjetividad en la valoración del operador jurídico.

No obstante, no puede desconocerse que las redes sociales disponen de unos códigos que van a tener que estar muy presentes en esta valoración. Por ejemplo, retuitear un mensaje no siempre significa estar de acuerdo con su contenido sino que, por el contrario, a veces la intención de emisor es denunciar el mensaje.

Además, tampoco puede ocultarse que estos códigos no siempre están claros ni son por todos conocidos, de forma que la valoración de la intención del emisor del mensaje, en ocasiones, deberá evaluarse a partir del conjunto de sus mensajes y no aisladamente.

### 2.3. ¿Quién emite el mensaje?

El tercer elemento a valorar según el TEDH es quién es el emisor del mensaje. En coherencia con su jurisprudencia que concibe la libertad de expresión como fundamento del sistema democrático, la Corte defiende una mayor protección de los mensajes difundidos por los políticos y por los medios de comunicación.

En el primer caso, la posibilidad de restringir la libertad de expresión de los políticos es reducida, como se explica en la Sentencia *Incal v. Turquía* (1998), donde se analizaba la condena a un miembro del comité ejecutivo del Partido Popular de los Trabajadores por haber contribuido a preparar unos panfletos de propaganda separatista. La Corte repitió que la libertad de expresión es particularmente importante en el ámbito de los partidos políticos y sus miembros, pues representan a su electorado y fijan la atención en sus preocupaciones e intereses; de acuerdo con ello, la restricción a la libertad de expresión de un político del partido de la oposición al gobierno, como era el demandante, llamaba a un mayor escrutinio por parte de la Corte. No obstante, cabe señalar que esta jurisprudencia convive con sentencias como la *Erbakan v. Turquía* (2006), donde el TEDH sostiene que la libertad de expresión tampoco es absoluta para los políticos y enfatiza que es crucial que estos no difundan en sus discursos públicos comentarios susceptibles de alimentar la intolerancia.

Respecto a la mayor protección de los medios de comunicación, la cuestión esencial radica en discernir el papel del periodista, editor o propietario del medio de comunicación, como autor del mensaje o como mero agente que lo difunde. Ya se ha hecho alusión a esta distinción, que supuso la protección del periodista que entrevistó a un grupo de jóvenes racistas denominado *The Greenjackets* (*Jersild v. Dinamarca*, 1994), pero que no protegió en cambio al propietario de una revista por el contenido de dos cartas al director (*Sürek v. Turquía*, 1999).

Desde la perspectiva del emisor del mensaje, ya se ha destacado que en el ámbito de la comunicación en red se plantea en ocasiones el asunto de su difícil identificación. ¿En qué medida supone esto un problema para la determinación de los límites de la libertad de expresión en la red? ¿La incertidumbre sobre quién es el emisor impide que pueda aplicarse este parámetro a las redes sociales?

Parece que la respuesta debe ser negativa. En el caso de que sea imposible la identificación del emisor, la valoración sobre la adecuación del mensaje se realizará sin aplicar el parámetro de la mayor protección a los políticos y a los medios de comunicación, puesto que no habrá quedado acreditado que estos son los emisores. En suma, la dificultad para identificar al emisor del mensaje que plantea la comunicación en red afecta escasamente a los límites de la libertad de expresión, pues simplemente dejará de aplicarse la especial protección ofrecida a ciertos grupos.

### 2.4. ¿A quién se dirige el mensaje?

El cuarto parámetro que emplea el TEDH es el colectivo destinatario del mensaje. En este punto, la Corte también es coherente con la especial protección que otorga al debate sobre asuntos públicos, pues considera que los límites de la crítica tolerable son más amplios cuando se dirige contra un político y menores cuando se centra en un individuo particular. A diferencia del ciudadano particular, el político está sometido a un mayor escrutinio tanto por la prensa como por la sociedad en general y, por tanto, debe ser más transigente ante las críticas (*Lingens v. Austria*, 1986). Ello incluye a los gobiernos, puesto que sus acciones y omisiones están igualmente sujetas a un atento escrutinio, no solo del poder legislativo y judicial, sino también por parte de la prensa y la opinión pública (*Castells v. España*, 1992).

De nuevo, parece que este parámetro puede aplicarse miméticamente a la comunicación en red, de forma que el destinatario del mensaje deberá ser tenido en cuenta cuando se valora la libertad de expresión en las redes sociales. Así, los mensajes críticos contra los políticos disfrutarán de una mayor protección.

## 2.5. ¿Por qué canal se difunde el mensaje?

El quinto parámetro hace referencia a los canales utilizados para difundir el mensaje. En este contexto, el TEDH analiza el tipo de programa donde este se emite: en *Jersild v. Dinamarca* (1996), la Corte tuvo en cuenta que el mensaje se difundió en un programa de noticias serio y dirigido a una audiencia bien informada; y en *Gündüz v. Turquía* (2003), la Corte ampara unas apreciaciones del demandante que podían ser consideradas como insultantes por haberlas realizado durante una retransmisión televisiva en directo, de manera que no tuvo posibilidad de reformularlas, redefinirlas o retractarse de las mismas al pronunciarlas.

En este contexto resulta relevante reseñar que la Corte pone en conexión la expresión artística con los canales de difusión del mensaje, por considerar que en muchos casos el grado de divulgación de las creaciones artísticas es menor. Al parecer del TEDH, expresiones artísticas como la poesía tienen un impacto inferior al de los medios de comunicación social, pues por su naturaleza interesan a un limitado número de personas; esta menor difusión juega a favor de su amparo en el artículo 10 del Convenio (*Karata v. Turquía*, 1999).

Aquí sí nos encontramos con un parámetro que puede obligar a valorar de modo diferente la comunicación en red y la realizada a través de medios más tradicionales. ¿Cuáles son los datos relevantes a tener en cuenta cuando se evalúa el canal de difusión del mensaje según la jurisprudencia europea? La mayor protección de los programas de noticias serios, dirigidos a un público informado; de la emisión de mensajes en directo; y de los mensajes críticos plasmados en creaciones artísticas por su escasa difusión.

Los datos relevantes son, pues, la seriedad del programa, la inmediatez y el grado de difusión.

Respecto de la seriedad, cabe traer a colación de nuevo aquí que se ha defendido una supuesta menor seriedad en

los contenidos vertidos en las redes sociales, dada la pluralidad de emisores y su menor profesionalidad respecto de los medios de comunicación tradicionales. No se van a valorar aquí afirmaciones de estas características, que quizás no tienen del todo presente la falta de seriedad de los mensajes emitidos, en ocasiones, en los canales tradicionales de comunicación; además, puede considerarse que no todas las redes sociales gozan del mismo nivel de credibilidad. En todo caso, la comunicación en red quizás no merezca una mayor protección como pueden merecer otros formatos comunicativos emitidos por medios más convencionales; no obstante, tampoco puede desprenderse de la jurisprudencia europea que deba penalizarse a la comunicación en redes sociales por su supuesta falta de seriedad.

Respecto de la inmediatez, se ha comprobado que el TEDH considera que juega a favor del emisor del mensaje. Este dato favorece a ciertas redes sociales cuyo valor se fundamenta en la rápida reacción o respuesta a determinados acontecimientos o mensajes previos. Aunque también aquí cabe insistir en que la Corte valora la capacidad de retractarse del emisor ante un mensaje inadecuado; esta capacidad resulta más sencilla y rápida en la red y, por tanto, parece más exigible que en los canales convencionales.

Finalmente, el grado de difusión del mensaje es otro dato fundamental. No cabe duda de que una de las características más destacables de la comunicación a través de redes sociales es que los mensajes pueden alcanzar un elevado grado de difusión. Ello no jugará a favor del emisor de un mensaje inapropiado si se constata que usó la red con la intención de dar la mayor publicidad a su mensaje. No obstante, si se produce una mayor difusión por haberse utilizado la red y, como consecuencia, un efecto más dañino que si el mensaje se hubiera difundido por otros canales, la valoración de este dato será igual que si idéntica difusión y perjuicio se hubieran producido a través de los medios convencionales.

## 2.6. ¿En qué lugar se emite el mensaje?

Finalmente, según el TEDH, el lugar donde se emite el mensaje es otro parámetro para determinar los límites de la libertad de expresión. Lo que la Corte evalúa aquí es la relevancia de la materia en un lugar geográfico concreto, lo cual tiene implicaciones en el mayor o menor grado de limitación de esta libertad.

La valoración de este parámetro ha sido habitual en los casos relativos a Turquía, concretamente, en los temas ligados a la lucha contra el terrorismo, donde se otorga un amplio espacio para la limitación de la libertad de expresión. Son elocuentes las ocho sentencias dictadas en el caso *Bayar v. Turquía* (2014), donde la Corte explica que es plenamente consciente de las dificultades que afronta el Estado turco en la batalla contra el terrorismo, aunque concluye enfatizando también la relevancia de la libertad de expresión y otorgando el amparo al demandante, fundamentalmente, por considerar que no se incitaba a la violencia.

En relación con Francia, sirve de ejemplo la Sentencia *Jean-Marie Le Pen v. Francia* (2010), donde se evaluaban los mensajes contra los inmigrantes proferidos por el fundador del partido Frente Nacional, quien sostuvo que «el día en que en lugar de cinco millones (de musulmanes) sean veinticinco, ellos estarán al mando». En esta ocasión, la Corte no amparó al político francés e insistió en el problema específico que existe en este país en relación con la inmigración y el mayor margen que ello implicaba para limitar su libertad de expresión.

Como resulta obvio, el lugar es irrelevante en el caso de la comunicación a través de redes sociales. Otra de las características más destacables de la comunicación en red es su transversalidad geográfica, que al mismo tiempo plantea el problema de la diferente consideración que puede tener el mismo mensaje en un lugar u otro.

### 3. ¿Deben tratarse de modo diferente los mensajes emitidos en las redes sociales?

Durante muchas décadas, se ha producido un intenso debate sobre los límites de la libertad de expresión, que ha ido parejo a acontecimientos relacionados con cambios en las formas de comunicación social y, también, con otros

fenómenos totalmente ajenos a esta libertad pero con una influencia directa como, en la actualidad, el terrorismo internacional.

En este contexto, la irrupción de las redes sociales como nueva forma de comunicación social plantea el siguiente interrogante: ¿dónde se sitúan los límites de los contenidos que circulan por la red?

Puede sostenerse que la percepción generalizada es que, con las redes sociales, la libertad de expresión parece ganar espacio. Los motivos que contribuyen a esta percepción son diversos: por un lado, las tecnologías y la expansión de los códigos parecen ilimitadas; por otro lado, se ha producido una clara ruptura de las barreras territoriales y temporales; finalmente, la era del *big data* contribuye a generar el efecto de ilimitado acceso y de ilimitada libertad.<sup>10</sup> Además, el público ya no está abocado a recibir pasivamente mensajes, sino que ahora también puede interactuar con los mismos, modificarlos o interpretarlos individualmente o en colaboración con otros usuarios de las redes de comunicación, generando informaciones u opiniones propias e incluso convirtiéndose en fuente para los medios de comunicación social.<sup>11</sup>

Del escenario que acaba de dibujarse ha llegado a derivarse la conveniencia de una suerte de discriminación positiva para la comunicación en red, algo que podría plantearse en atención a los muy significativos beneficios que su desarrollo y potenciación pueden deparar desde la perspectiva de la consecución de un mayor pluralismo.<sup>12</sup>

Contrariamente, en la práctica, se ha defendido que la exagerada percepción de riesgos asociados a la generalización de la comunicación en red y la multiplicación de emisores y receptores han permitido que se haya aceptado socialmente tanto un incremento de las posibilidades de represión del pensamiento disidente, rebajando la sensibilidad de los mecanismos de represión penal en estos casos, como la aparición de procedimientos directos e indirectos de control administrativo de la expresión que habían desaparecido. El hecho de que no se controle

10. Esta percepción y los motivos que han llevado a ella han sido tomados de Rodríguez-Amat et al. (2013, pág. 76 y 78).

11. Así lo explica Boix (2002, pág. 89).

12. Así lo defiende Boix (2002, pág. 106). No obstante, más allá de alguna referencia pasajera a esta teoría, este autor aboga por la igualdad de los límites de expresión en la comunicación en red y en la llevada a cabo a través de los medios tradicionales de comunicación (2002, pág. 133-134).

a medios de comunicación sino a usuarios individuales, y que estos controles no sean particularmente molestos para las propias redes sociales que dan soporte a estos intercambios, ni limiten excesivamente su negocio, hacen que la reacción frente a estas restricciones resulte más complicada.<sup>13</sup>

Más allá de percepciones sociales sobre el mayor espacio de la libertad de expresión en la red o de tesis que sostienen una mayor represión y control de los contenidos difundidos en las redes sociales, lo que importa aquí es analizar jurídicamente si existen argumentos que justifiquen una diferenciación de los límites de la libertad de expresión cuando esta se ejercita en la red o a través de canales de comunicación convencionales.

Para responder a esta cuestión, debe comenzarse por determinar cuáles son los elementos que diferencian la comunicación en red respecto de la comunicación por canales tradicionales. Como se ha detallado, pueden contabilizarse hasta cuatro elementos distintivos desde la perspectiva de los límites a la libertad de expresión: la posición del receptor del mensaje, que puede en cualquier momento interactuar respecto del mismo y convertirse en emisor (a veces anónimo o poco fiable); la posición de relativa igualdad del emisor del mensaje; la gran cantidad y variedad de contenidos en la red; el aumento de la capacidad de interrelación comunicativa, que a su vez provoca una mayor exposición pública; y la indelebilidad de los mensajes.

El siguiente paso consiste en repasar cuáles son los límites clásicos de la libertad de expresión para confrontarlos con estos elementos distintivos de la comunicación en red. En otras palabras, debe analizarse si estos límites pueden aplicarse *mutatis mutandi* a un modo de comunicación distinto al tradicional cual es la comunicación a través de redes sociales. Los límites clásicos de la libertad de expresión han sido establecidos por el TEDH, que emplea unos parámetros concretos para decidir si un mensaje debe recibir protección.

Los parámetros europeos que se han considerado relevantes para este análisis han sido los siguientes: la materia sobre la que versa el mensaje; la intención del emisor;

quién emite el mensaje; a través de qué canal; y el ámbito geográfico donde se difunde.

Comenzando por la materia difundida, y en coherencia con la concepción de la libertad de expresión como fundamento del sistema democrático, el TEDH ha realizado una suerte de jerarquización de contenidos al defender la mayor protección de los relacionados con la política o con asuntos de interés público, frente a los que se alejan de estas materias. Este criterio puede aplicarse sin fisuras a los mensajes en red. Es más, resulta especialmente conveniente dada la enorme variedad de materias que circulan por las redes sociales, pues permite graduar la protección a la libertad de expresión en la red en función del contenido sobre el que versa el mensaje.

El parámetro relativo a la intención del emisor implica preguntarse si este trató de difundir mensajes, por ejemplo, xenófobos, o si, por el contrario, trataba de informar sobre asuntos de interés general. También este baremo puede emplearse en la comunicación en red, observando los elementos que permiten traslucir cuál ha sido la voluntad del emisor. La única precisión que en este punto debe hacerse es que, en el caso de los mensajes difundidos en redes sociales, deberán tomarse en consideración los códigos o usos habituales en este tipo de comunicación, no siempre claros ni por todos conocidos dada su relativa novedad.

El TEDH también usa como parámetro quién es el emisor del mensaje y, de nuevo en coherencia con su concepción de la libertad de expresión como fundamento del sistema democrático, la Corte defiende una mayor garantía de los mensajes difundidos por los políticos y por los medios de comunicación. El único inconveniente para aplicar este criterio a la comunicación en red podría ser la dificultad para identificar al autor del mensaje; no obstante, esta dificultad se desvanece puesto que, cuando se desconozca al autor, simplemente dejará de aplicarse la mayor protección del mensaje.

La persona o colectivo destinatario del mensaje es otro parámetro a valorar según la Corte, que ha defendido el mayor margen para la libertad de expresión cuando se debate sobre políticos en coherencia otra vez con su función en el sistema democrático. Parece que este criterio puede

13. De esta opinión es Boix (2016, pág. 196).

aplicarse sin complicaciones a la comunicación en red, que quedará especialmente garantizada si el mensaje se refiere a la clase política.

El contexto geográfico donde se difunde el mensaje también es un parámetro a evaluar en el momento de trazar los límites de la libertad de expresión: según la Corte, las restricciones pueden ser mayores si se abordan asuntos que en un ámbito geográfico concreto resultan delicados o conflictivos. Desde la perspectiva de la comunicación en red, y dada su transversalidad geográfica, este baremo carece de peso específico.

Hasta aquí, los parámetros empleados por el TEDH en la comunicación a través de los canales tradicionales pueden aplicarse casi sin matices a la comunicación en red. En cambio, el que se expone seguidamente reúne unas connotaciones diferentes.

El canal a través del cual se emite el mensaje es otro baremo utilizado por el TEDH. En relación con el mismo, la Corte considera que en el momento de trazar los límites de la libertad de expresión juegan a favor de esta libertad: la seriedad del programa en el cual se vierten los mensajes, la inmediatez de la comunicación y su menor grado de difusión.

Resulta palmario que estas tres variables tienen una relevancia especial en el campo de la comunicación en red, por lo que merecen ulteriores consideraciones.

En primer lugar, se ha defendido la menor seriedad de los mensajes vertidos en las redes sociales. No obstante, si eventualmente ese fuera el caso, bastaría con no proteger especialmente estos mensajes, pero no justificaría penalizarlos o desnudarlos de garantías.

En segundo lugar, la inmediatez juega a favor del mensaje, lo cual favorece la comunicación a través de determinadas redes sociales. No obstante, también debe puntualizarse que la Corte evalúa la capacidad de retractarse del emisor ante un mensaje inadecuado y que esta capacidad resulta más sencilla y rápida en las redes, con lo que será más exigible que en los canales más convencionales.

Finalmente, en ocasiones la difusión de los mensajes en red es mucho mayor que a través de otros canales más convencionales. Como consecuencia, la emisión de mensajes inapropiados por aquella vía no jugará a favor del emisor si se constata que usó la red con la intención de dar mayor publicidad a su mensaje. No obstante, si se produce una mayor difusión por haberse utilizado la red y, como resultado, un efecto más dañino que si el mensaje se hubiera difundido por otros canales, la valoración de este dato será igual que si idéntica difusión y perjuicio se hubieran producido a través de los medios convencionales.

En suma, si se analizan los parámetros empleados por el TEDH para trazar los límites a la libertad de expresión y se aplican a la comunicación en red, se observa que en su mayor parte pueden aplicarse *mutatis mutandi*. El único baremo que requiere un trato especial es el relativo al canal a través del cual se emite el mensaje, donde la Corte evalúa la seriedad del canal, su inmediatez y grado de difusión; no obstante, este parámetro puede aplicarse a los mensajes en red de forma muy análoga a los emitidos en canales convencionales.

Así, puede concluirse que jurídicamente no deberían trazarse unos límites distintos a la libertad de expresión en función de si el mensaje se difunde o no a través de redes sociales.

## Bibliografía

- BOIX, A. (2016). "La construcción de los límites a la libertad de expresión en las redes sociales". *Revista de Estudios Políticos*, n.º 173, pág. 55-112.
- BOIX, A. (2002). "Libertad de expresión y pluralismo en la red". *Revista Española de Derecho Constitucional*, n.º 65, pág. 133-180.
- BOIX, A.; LÓPEZ GARCÍA, G. (2005). "Derecho y cuarto poder en la era digital". *Revista de Estudios Políticos*, n.º 130, pág. 77-112.
- CARRILLO, M. (2013). "Internet como espacio público de la información". En: P. REQUEJO (ed.). *Derechos y espacio público*. Universidad de Oviedo y Procuradora General del Principado de Asturias, Oviedo, pág. 11-28.



- COLE, D. (2012). "The First Amendment' borders: the place of Holder v. Humanitarian Law Project in First Amendment Doctrine". *Harvard Law Review and Policy Review*, n.º 6, pág. 147-177.
- DÍEZ BUESO, L. (2002). "La relevancia pública en el derecho a la información: algunas consideraciones". *Revista Española de Derecho Constitucional*, n.º 66, pág. 213-238.
- LEZERTÚA, M. (1993). "El derecho a la libertad de expresión en la jurisprudencia de la Comisión y del Tribunal Europeo de Derechos Humanos". En: VV.AA., *La jurisprudencia del Tribunal Europeo de Derechos Humanos*. Consejo General del Poder Judicial. Madrid.
- LÓPEZ GARCÍA, G. (2005). *Modelos de comunicación en Internet*. Valencia: Tirant lo Blanch.
- MUÑOZ MACHADO, S. (2000). *La regulación de la red. Poder y Derecho en Internet*. Madrid: Taurus.
- ROBLES, J.M.; MOLINA, O.; DE MARCO, S. (2012). "Participación política digital y brecha digital política en España. Un estudio de las desigualdades digitales". *ARBOR Ciencia, Pensamiento y Cultura*, vol. 188, pág. 795-810.
- RODRÍGUEZ-AMAT, J.R.; SARIKAKIS, K.; GANTER, S.A. [et al.] (2013). "Gobernanza de Internet y libertad de expresión en Europa: estado de la cuestión". En: L. CORREDOIRA y L. COTINO (dirs.). *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*. Centro de Estudios Políticos y Constitucionales. Madrid.
- TULKENS, F. (2012). "When to say is to do: freedom of expression and hate speech in the case-law of the European Court of Human Rights". En: *Freedom of expression. Essays in Honour of Nicolas Bratza, Oisterwijk*. Estrasburgo: Wolf Legal Publishers-Council of Europe.
- WEBER, A. (2009). *Manual on hate speech*. Council of Europe Publishing.

### Cita recomendada

DÍEZ BUESO, Laura (2018). «La libertad de expresión en las redes sociales». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 5-16. UOC [Fecha de consulta: dd/mm/aa]  
 <<http://dx.doi.org/10.7238/idp.v0i27.3146>>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (IDP. *Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

---

### Sobre la autora

Laura Díez Bueso  
lauradiez@ub.edu

Profesora de Derecho Constitucional  
Facultad de Derecho (UB)  
<[http://www.ub.edu/dconst/membres/docs/Curriculum%20L\\_Diez.pdf](http://www.ub.edu/dconst/membres/docs/Curriculum%20L_Diez.pdf)>

Facultat de Dret  
Avda. Diagonal 684  
08034 Barcelona  
Despatx 302 - Ed. Ilerdense



**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## ARTÍCULO

# Los delitos de odio en las redes sociales

Josep M. Tamarit Sumalla  
 Catedrático de Derecho penal (UOC)

Fecha de presentación: mayo de 2018  
 Fecha de aceptación: julio de 2018  
 Fecha de publicación: septiembre de 2018

## Resumen

Las redes sociales presentan características idóneas para el incremento del riesgo de conductas de relevancia penal y los delitos de odio son un ámbito afectado por la expansión del Derecho penal. Sin embargo, los tribunales españoles no responden de un modo consistente y predecible, mostrando una severidad en la aplicación del tipo delictivo de enaltecimiento del terrorismo que constituye una amenaza para el derecho a la libertad de expresión y para el principio de proporcionalidad de las penas. El trabajo analiza la jurisprudencia del Tribunal Supremo y concluye proponiendo la necesidad de recuperar el modelo liberal del CP 1995 y que la jurisprudencia evolucione según las directrices derivadas de la Corte Europea de Derechos Humanos para situar, en su lugar adecuado, la respuesta ante el discurso del odio.

## Palabras clave

delito de odio, discriminación, libertad de expresión, provocación, redes sociales, xenofobia

## Tema

delitos de odio

## *Hate crimes on social networks*

## Abstract

*Social networks have suitable characteristics for the increase of criminal behaviours, with hate crimes being one area affected by the expansion of Criminal Law. However, the Spanish courts do not respond in a consistent and predictable manner, acting harshly in the application of the crime of glorifying terrorism, which constitutes a threat for the right to freedom of expression and for the principle of*

*sentence proportionality. The study analyses the jurisprudence of the Spanish Supreme Court and concludes by outlining the need to recover the liberal model of the criminal code of 1995, and for jurisprudence to evolve according to the European Court of Human Rights guidelines so that it can respond appropriately to hate speech*

### Keywords

*hate crime, discrimination, freedom of expression, provocation, social networks, xenophobia*

### Topic

*hate crimes*

## 1. Introducción

Los delitos de odio son un ámbito afectado por la expansión del Derecho penal. Este fenómeno se produce a la vez que se expande el uso masivo de las redes sociales. Todo ello pone a prueba la resistencia del viejo e ilustrado Derecho penal ante los embates del paternalismo punitivo y las actitudes temerosas con formas de expresión más informales y desinhibidas que se imponen entre las personas jóvenes. En este contexto, algunos autores advierten sobre la necesidad de defender los principios fundamentales de protección de bienes jurídicos o de lesividad, en la versión propia de la tradición germánica, o el *harm principle* o *offence principle* de la tradición angloamericana (Miró Linares, 2015). La expansión de los delitos de odio puede ser vista así como el resultado de un proceso histórico de inversión. Una vez superada la funesta etapa en que el Derecho penal se utilizaba como brazo ejecutor de una sociedad intolerante contra los derechos de las minorías, los principios liberales se ven ahora amenazados por una utilización abusiva de instrumento punitivo al servicio de la voluntad de defender a esas minorías, con el riesgo de que la inversión llegue al punto de una aplicación perversa de estas nuevas tipologías delictivas, utilizadas contra los intereses de las propias minorías a las que deberían servir.

Conocer la realidad de los delitos de odio en España es difícil dadas las deficiencias de los datos oficiales y la casi inexistencia de encuestas generales de victimización. Desde 2013, el Ministerio del Interior incluye en su Anuario un capítulo dedicado a estas infracciones, que publica además como documento independiente: el «Informe sobre la evolución de los incidentes relacionados con los delitos de odio en España». Según el Informe de 2016,<sup>1</sup> se registraron 1.272 hechos calificados policialmente como delitos de odio. Las víctimas de estos hechos fueron en un 62 % hombres (789) y en un 36 % mujeres (468), un 73 % de nacionalidad española y un 27 % extranjeros. La comunidad autónoma con un mayor número de denuncias fue Cataluña, con 282 (el 22 % del total), seguida de lejos por Madrid, con 171.<sup>2</sup> Los delitos denunciados son la punta del iceberg de una realidad que en su mayor parte no llega a ser conocida oficialmente, en especial por el sistema de justicia penal.<sup>3</sup> El Informe recoge específicamente datos referidos al discurso del odio, con un total de 124 casos, en su mayor parte motivados por la ideología (44), el racismo o la xenofobia (22), la discapacidad (22) y la orientación o identidad sexual (21). Estos hechos habrían sido cometidos a través de internet en un 42 %, telefonía en un 21% y redes sociales en un 15,4 %.<sup>4</sup>

1. <<http://www.interior.gob.es/documents/10180/5791067/ESTUDIO+INCIDENTES+DELITOS+DE+ODIO+2016.pdf/c5ef4121-ae02-4368-ac1b-ce5cc7e731c2>>.
2. Esta cifra relativamente elevada, superior al peso demográfico de Cataluña en el conjunto del Estado, puede ser el resultado de la labor llevada a cabo por el fiscal especial para delitos de odio en Barcelona y el grupo especializado de los Mossos d'Esquadra, que habría hecho aflorar un mayor número de casos.
3. Uno de los problemas frente a los delitos de odio es precisamente la baja tasa de denuncias. Un indicio de ello estaría en la Encuesta de seguridad pública de Cataluña, cuya última edición publicada (2015) por primera vez ha incluido una pregunta en los casos de agresión referida a los motivos. El resultado es que en un 12 % de casos habría habido un motivo de género y en un 12 % un motivo ideológico.
4. Resulta dudoso a qué se refiere el grupo más numeroso de casos, designado como internet. Asimismo, resulta poco esclarecedor el dato referido al tipo de delito, ya que el grupo más numeroso de casos corresponde a «otros».

Por otra parte, la Fiscalía General del Estado, en sus memorias anuales, aporta información sobre la actividad de los fiscales delegados para delitos de odio. Según la Memoria de 2017, en 2016 se incrementaron las denuncias por delitos de odio a través de internet y las redes sociales, pasando los procedimientos incoados de 40 (en 2015) a 99. Una parte importante de este incremento corresponde a los contenidos ilícitos encuadrables en el discurso del odio.<sup>5</sup> El dato diverge de la evolución reflejada en el Informe del Ministerio del Interior, según el cual las denuncias disminuyeron entre 2015 y 2016. En cuanto a las sentencias por delitos de odio, la Memoria refleja una tasa de condena que se situaría en torno al 20 %, respecto al total de hechos denunciados, con tan solo 35 sentencias condenatorias,<sup>6</sup> 16 por delitos en los que se apreció la agravante del artículo 22-4 CPE y 11 por delito de trato degradante (artículo 173). No se recogen datos de cuántos delitos estarían relacionados con las redes sociales, aunque es fácil deducir que serían pocos. Tan solo se registran tres casos del artículo 510 y no aparecen registrados los de enaltecimiento del terrorismo (578).<sup>7</sup>

Es bien sabido que las redes sociales presentan características que incrementan el riesgo de conductas de relevancia penal, como el anonimato (García González, 2015), la desinhibición o el desarrollo de una identidad disociativa (Agustina, 2014; Tamarit, 2018). Asimismo, la facilidad de comunicación y la extensión del círculo de relaciones interpersonales generan crecientes oportunidades (Miró Linares, 2011). Desde la perspectiva de los ofensores, determinadas características de personalidad, como las relacionadas con la impulsividad, suponen un incremento del riesgo, del mismo modo que el comportamiento de la víctima, concretamente su mayor participación en las redes sociales, la expone a un mayor riesgo de ser objeto de expresiones lesivas para sus bienes jurídicos. Todo ello plantea interpelaciones a la dogmática jurídico-penal, que desbordan los límites de este trabajo, como la relevancia que puede tener el comportamiento de la víctima en internet en la valoración de la necesidad de intervención penal

o, en su caso, cómo debería medirse la culpabilidad de quienes actúan impulsivamente o qué papel debería tener el argumento víctima-dogmático en los casos en que los participantes adoptan a la vez un rol de ofensor y víctima.

Vamos a examinar seguidamente los aspectos esenciales del tratamiento jurídico-penal de los delitos de odio que tienen mayor relevancia en relación con la actividad desarrollada en las redes sociales, para abordar después un análisis de la jurisprudencia del Tribunal Supremo al objeto de conocer los criterios que determinan la aplicación judicial de los diversos tipos delictivos.

## 2. Los delitos de odio y la expansión del Derecho penal

Los delitos de odio suponen la realización de una conducta delictiva mediante la cual el autor expresa un mensaje de odio o discriminación hacia un grupo social. Una característica esencial de esta clase de delitos es que la víctima es seleccionada por el autor como consecuencia de una adscripción social que lo vincula a un determinado grupo. Es esa adscripción, derivada de su origen nacional o étnico u otras circunstancias relacionadas con su identidad, como el género o la orientación sexual o la ideología, la que convierte a la víctima en un objetivo atractivo para el autor. Asimismo, el grupo social al que, desde la percepción del autor, está vinculada la víctima directa es destinatario del mensaje discriminatorio y víctima indirecta del hecho.

La investigación criminológica ha señalado que un elemento intrínseco a esta experiencia de victimización es el mensaje intimidatorio, en que las características individuales de la víctima no son relevantes en comparación con el significado social que esta tiene. El objeto de la agresión por odio no es lo que la víctima es individualmente, sino lo que representa (Garland, 2011). Según algunos enfoques, las ideas de jerarquía y dominación son inherentes a la

5. Así lo destacaron fuentes de la FGE: <<http://www.europapress.es/epsocial/igualdad/noticia-fiscalia-alerta-incremento-delitos-odio-traves-internet-redes-sociales-2016-20170905130511.html>>.
6. La Memoria no explicita que sean condenatorias, aunque así cabe deducirlo de que se informe de 82 casos en los que la Fiscalía formuló acusación (Memoria FGE 2017, pág. 743).
7. En otro orden, la Memoria pone en cuestión la carencia de un sistema informático que permita una mejor gestión y coordinación de la persecución contra estos delitos y resalta la importancia de la relación entre los fiscales delegados y las organizaciones sociales dedicadas a combatir estos delitos.

victimización por odio, pues la violencia se ejerce como expresión de la actitud social hegemónica que perpetúa la subordinación de ciertos grupos y es una violencia «punitiva» que tiene una función de recordar a los miembros de estos grupos la posición que les corresponde en la sociedad (Perry, 2009). Esta perspectiva ha sido discutida con el argumento de que no se adecúa a la violencia y los abusos que tienen como objeto personas con discapacidad, ancianas o sin hogar, en las que la selección de estas como objetivos tiene que ver con el hecho mismo de su vulnerabilidad y de que se adecúan más a la imagen social de la «víctima ideal» (Chakraborti y Garland, 2012).

Por otra parte, la investigación victimológica ha estudiado hasta qué punto el componente de odio de un delito supone un daño adicional para la víctima. Un estudio elaborado a partir de la Encuesta británica de victimización reveló que muchas víctimas de delitos de odio sufren un mayor impacto emocional que las de similares delitos sin esta clase de motivación (Karmen, 2013). Sin embargo, ello no puede afirmarse de todas ellas, por lo que no son recomendables respuestas jurídicas o institucionales estereotipadas basadas en presunciones. Por otra parte, en comparación con otros delitos sin motivación discriminatoria, las víctimas de delitos de odio muestran mayor propensión a sufrir miedo, niveles elevados de depresión, ansiedad, pérdida de confianza, insomnio y reducción de los niveles de bienestar (Iganski y Lagou, 2015). Para comprender este impacto diferencial del delito de odio, debe tenerse en cuenta la dimensión social inherente a la victimización. Así, por ejemplo, para una persona que sufre un ataque racista por el hecho de sus orígenes, el delito no significa tan solo la agresión y las posibles lesiones derivadas, sino el recordatorio doloroso de la herencia cultural de discriminación y estigmatización de su grupo.

### 3. Provocación al odio y discurso del odio

La regulación positiva de los delitos de odio en el Código penal español (CPE) se centra, fundamentalmente, en la circunstancia agravante del artículo 22-4 y en el delito de provocación al odio y la discriminación del artículo 510. Esta figura delictiva fue objeto de una profunda reforma mediante la LO 1/2015, caracterizada por una gran expansión del ámbito de conductas típicas. Además, se

añadió al citado precepto el tipo delictivo de justificación del genocidio (anterior artículo 607-2), adaptado a la STC 235/2007, de 7 de noviembre. La reforma trae causa de la Decisión marco 2008/913/JAI y guarda coherencia con la evolución seguida por las legislaciones de otros estados miembros. Esta evolución ha sido cuestionada desde sectores liberales, y en España también por un importante sector de la doctrina penal. Así, como muestra, Portilla Contreras (2015) ha afirmado que estos delitos «simbolizan el desprecio por la libertad de expresión, creencia e ideología».

El artículo 510-1 CPE describe tipos delictivos, referidos a las conductas previstas en la DM 2008/913/JAI, relativa a la lucha contra determinadas formas y manifestaciones del racismo y la xenofobia mediante el Derecho penal: a) la incitación al odio, b) la producción, elaboración o posesión de materiales idóneos para fomentar el odio; y c) la negación, trivialización o enaltecimiento del genocidio y delitos afines. El 510-2 describe además hechos típicos que van más allá de los supuestos previstos en la DM, para los que prevé penas de menor gravedad. La versión reformada del artículo 510 incluye en el ámbito de lo típico los supuestos de incitación indirecta, remite en primer lugar al odio y la hostilidad y refiere estos sentimientos, así como la violencia o discriminación provocada, no solo a un grupo sino a personas individuales por razón de su pertenencia a tal grupo. Esta ampliación responde a la preocupación ante los fracasos derivados de pronunciamientos absolutorios basados en la falta de prueba respecto a que el mensaje de odio tuviera como destinatario a todo un colectivo. En esta clave deben entenderse las presiones que se ejercieron en el proceso legislativo para tipificar de modo explícito la provocación indirecta, lo cual ha suscitado críticas por su antagonismo con una concepción liberal del derecho penal. El legislador de 2015 también ha ido más allá de los mínimos de penalización previstos por la DM al incluir otros motivos de discriminación, como la situación familiar, el sexo, la orientación o identidad sexual o por razones de género, enfermedad o discapacidad.

La provocación debe ser interpretada según el sentido del artículo 18 CPE, exigiendo que la conducta se lleve a cabo ante una concurrencia de personas o por algún medio que garantice la publicidad, tal como expresamente requiere el tipo. La publicidad se dará también en las manifestaciones divulgadas mediante las TIC, no solo por su exposición en una web o blog de acceso abierto, sino también a través

de las redes sociales con acceso restringido a usuarios registrados, siempre que el mensaje pueda ser transmitido a un amplio y relativamente indeterminado número de personas, tal como se desprende de lo previsto en el artículo 18, que se refiere a un medio de eficacia semejante a una imprenta y a una «concurencia de personas». Es obvio que la capacidad de divulgación de ciertas redes sociales es incluso superior a la de una reunión con un gran número de personas.

Responde a la vocación expansiva y de adelantamiento de la barrera de protección la tipificación de la acción de facilitar a terceros el acceso, con lo que probablemente se pretendía combatir la propagación del «discurso del odio» a través de webs, pero tiene como efecto la elevación a delito de conductas materialmente constitutivas de cooperación con un acto preparatorio de un acto preparatorio. Dada la amplitud del tipo, la definitiva determinación del carácter delictivo de los hechos dependerá, básicamente, del control de idoneidad que deberá efectuar el órgano jurisdiccional sobre la base de los elementos probatorios disponibles y valorando si el contenido de los materiales es idóneo para fomentar, promover o incitar, directa o indirectamente, al odio, la hostilidad, discriminación o violencia, referidos estos al mismo ámbito de sujetos previstos en la letra a) del artículo 510. La capacidad de restricción de lo típico de esta cláusula de adecuación es mínima, pues el tipo delictivo no exige una idoneidad concreta en función de un contexto y de destinatarios determinados -como en los tipos del artículo 510-1,a) o del artículo 510-1,c)-, sino una idoneidad abstracta, que básicamente deriva del propio contenido de los materiales sometidos al proceso judicial.<sup>8</sup>

El artículo 510-6 dispone con carácter preceptivo una nueva pena, consistente en la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos o cualquier clase de soporte objeto del delito o por medio de los cuales se hubiera cometido. El juez o tribunal sentenciador deberá, además, ordenar la retirada de los contenidos cuando el delito se hubiera cometido a través de las TIC. El control puede llegar en estos casos hasta el punto

de ordenarse el bloqueo del acceso o la interrupción de la prestación del mismo, si el tribunal aprecia que a través de un portal se difunden contenidos delictivos de modo exclusivo o preferente. Esta intervención, reclamada por significativos sectores sociales y profesionales para poder evitar la propagación del discurso del odio, es cuestionada desde un sector de la doctrina penal, llegando a ser calificada por Portilla Contreras (2015) como una forma de censura propia de un Estado autoritario.

La reciente tendencia a la aplicación de los delitos de odio más allá del ámbito de la protección de colectivos históricamente discriminados viene a confirmar las preocupaciones de las voces críticas ante la expansión legislativa. El inicio de procedimientos judiciales contra personas acusadas de lanzar insultos y mensajes hostiles contra policías sería un ejemplo de hasta dónde puede llegar una «aplicación inversa» de discurso del odio. En un uso extenso de esta idea se llegaría a abarcar todo comportamiento de hostilidad, resistencia o incluso excesos gestuales o verbales respecto a adversarios políticos. La expansión se expresa también en la conversión en «discurso de odio», con efectos de exasperación punitiva, conductas anteriormente calificadas como delitos penalizados solo con penas de multa, como las injurias, los ultrajes a la nación o sus símbolos o las ofensas contra las instituciones, dando lugar a una perversa reintroducción por la vía de hecho del delito de desacato destipificado en 1995. Esta concepción expansiva y criminalizadora del discurso del odio ha sido ratificada por el propio Tribunal Constitucional, que en la STC 177/2015 de 22 de julio señaló: «Es obvio que las manifestaciones más toscas del denominado "discurso del odio" son las que se proyectan sobre las condiciones étnicas, religiosas, culturales o sexuales de las personas. Pero lo cierto es que el discurso fóbico ofrece también otras vertientes, siendo una de ellas, indudablemente, la que persigue fomentar el rechazo y la exclusión de la vida política, y aun la eliminación física, de quienes no compartan el ideario de los intolerantes». En esta resolución el TC aceptó que «quemar públicamente el retrato de los monarcas es un acto no solo ofensivo sino también incitador al odio, en la medida en que la cremación de su imagen

8. Un mayor potencial de restricción del tipo habría tenido la introducción de una cláusula de idoneidad para perturbar la paz pública, en la línea de lo sostenido por Gómez Martín (2012), pero la valoración de tal idoneidad no es posible introducirla por vía interpretativa, dado que la LO 1/2015 la ha incluido como elemento de cualificación punitiva (artículo 510-4). Con ello el legislador español ha ido más allá de la DM, según la cual los estados pueden optar por castigar las conductas solo cuando estas puedan producir una perturbación para el orden público o que resulten amenazadoras, abusivas o insultantes.

física expresa, de un modo difícilmente superable, que son merecedores de exclusión y odio». Esta posición mayoritaria (se emitieron tres votos particulares)<sup>9</sup> ha sido criticada por Alcácer Guirao (2016; 2018), quien ha rechazado la deriva hacia un peligroso uso abusivo del argumento del discurso del odio, que pone en cuestión el carácter preferente de que goza la libertad de expresión en la Constitución. Además la jurisprudencia constitucional es criticable por haber llevado la protección penal del Rey más allá de la protección reforzada de la que ya dispone a través de los tipos de delitos contra la Corona.<sup>10</sup> Esta posición ha sido finalmente desautorizada por la Corte Europea de Derechos Humanos, que en la sentencia de 13 de marzo de 2018 ha condenado a España por vulneración del derecho a la libertad de expresión. La Corte, por unanimidad, ha entendido la quema de la imagen del Rey como una forma de crítica política de la monarquía y del Reino de España como nación, que no puede ser castigada con pena de prisión en la medida que no entraña una incitación al odio o la violencia ni debe ser interpretada como expresión del discurso del odio.<sup>11</sup>

#### 4. Apología del terrorismo y ofensas a las víctimas

La respuesta penal a los delitos de odio pasa también por la aplicación del tipo delictivo de enaltecimiento del terrorismo y humillación de las víctimas del artículo 578 CPE. Esta figura delictiva fue introducida en el CPE mediante la LO 7/2000, de 22 de diciembre, con la cual se abrió paso a una reacción penal específica ante la apología del terrorismo, cuyo carácter típico dejaba de estar condicionado a la concurrencia de provocación al delito, en los términos del artículo 18 CPE. Posteriormente, la LO 2/2015, de 30 de marzo, ha introducido nuevos contenidos en el precepto dirigidos a reforzar la reacción penal, sin alterar los elementos básicos constitutivos del delito.

El artículo 578 CPE tipifica dos conductas: el enaltecimiento o justificación públicos de los delitos de terrorismo o de sus autores o partícipes, y la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares. Las dos conductas tienen prevista la misma pena, aunque algunos autores han destacado su «desigual significación» y «distinta lesividad». En estos términos, García Albero (2016) ha criticado que con la mixtura de ambas alternativas típicas el legislador ha pretendido legitimar, por proximidad, la punición de la apología no provocadora. Asimismo, este autor ha puesto de manifiesto la inconsistencia de la jurisprudencia, pues se han dictado sentencias condenatorias por hechos tan simples como hacer una pintada en un lugar público con el anagrama de ETA, al tiempo que se han producido fallos tanto de signo absolutorio como condenatorio frente a la exhibición de fotos de presos de ETA, en función de las circunstancias del contexto y su valoración, con delimitaciones imprecisas.

El TC, en la sentencia 112/2016, ha confirmado, también con votos particulares, la constitucionalidad del artículo 578 CPE, concluyendo que la penalización del enaltecimiento del terrorismo constituye una legítima injerencia en la libertad de expresión en la medida que pueda considerarse como manifestación del discurso del odio. Sin embargo, pese a esta reiterativa jurisprudencia constitucional, una adecuada interpretación de esta modalidad típica debe tener en cuenta la Directiva UE/2017/541, de 15 de marzo, sobre delitos de terrorismo. La norma europea prevé en su artículo 5 que «los Estados miembros adoptarán las medidas necesarias para garantizar que se tipifique como delito, cuando se cometa intencionadamente, el hecho de difundir o hacer públicos por cualquier otro medio, ya sea en línea o no, mensajes destinados a incitar a la comisión de uno de los delitos enumerados en el artículo 3, apartado 1, letras a) a i), siempre que tal conducta preconice directa o indirectamente, a través, por ejemplo, de la apología de actos terroristas, la comisión de delitos de terrorismo, ge-

- 
9. Los tres votos de los magistrados Adela Asúa, Fernando Valdés y Juan Antonio Xiol no cuestionan el hecho esencial de que el discurso del odio puede legítimamente ser considerado como un límite a la libertad de expresión, aunque se expresan en términos críticos frente a lo que Xiol califica como «banalización del discurso del odio» o, en términos de Asúa, «desfiguración» de tal discurso.
  10. El salto punitivo que supone llevar esta clase de conductas al ámbito del artículo 510 CPE es muy sustancial, ya que las injurias y calumnias al Rey tienen prevista una pena de prisión de seis meses a dos años si son graves y de multa si no lo son (artículo 490-3 CPE).
  11. Según la Corte, el derecho a la libertad de expresión tan solo podría ser limitado para castigar expresiones que propaguen, inciten, promuevan o justifiquen el odio fundado en la intolerancia, y mediante sanciones proporcionadas al fin perseguido, sin que la finalidad de proteger al Jefe del Estado sea razón suficiente para justificar un tal sacrificio.



nerando con ello un riesgo de que se puedan cometer uno o varios de dichos delitos». La exigencia de que concurra un riesgo, según la lógica propia de los delitos de peligro concreto, ajena al tenor literal del artículo 578 CPE, reclama de los tribunales una interpretación restrictiva que excluya del ámbito de lo típico los actos que, como mínimo, no tengan ese potencial lesivo.

La segunda modalidad típica del artículo 578 CPE (actos que entrañen descrédito, menosprecio o humillación de las víctimas) ha sido a veces interpretada como una forma especial de injuria, en tanto que ofensa al honor o a la dignidad de las víctimas. Sin embargo, esta interpretación debería llevar a criticar la previsión de una penalidad mucho más elevada que la del delito de injurias (artículo 209 CPE), que no va más allá de una pena de multa, pues suponer que una persona por el hecho de haber sido víctima tiene más dignidad u honor entraña una vulneración del principio de igualdad, al que se encuentra estrechamente vinculado el principio de dignidad humana. La diferencia punitiva debe explicarse, pues, indagando de otro modo el contenido de injusto de estas conductas, ante lo cual se plantean dos posibles vías. Por una parte, entender que el artículo 578 incrimina hechos que afectan a un bien jurídico de titularidad colectiva que expresa el significado político de las víctimas del terrorismo. Ello sería coherente con la naturaleza pública de este delito (a diferencia con el carácter privado de los delitos contra el honor), con el hecho de que las víctimas del terrorismo son las únicas que gozan de esta consideración penal y con la proclamación explícita de esta significación política efectuada en el preámbulo de la Ley 29/2011, de 22 de septiembre, de reconocimiento y protección integral de las víctimas del terrorismo. En la medida que sea este el criterio de aplicación del tipo delictivo deberían tenerse en cuenta las críticas ya conocidas a la manipulación política de las víctimas (Tamarit, 2013). Por otra parte, cabe una interpretación de base victimológica, que parte de la visión de las ofensas a quienes han sido víctimas como una forma de victimización secundaria. La victimología ha estudiado la exposición a ciertas imágenes e informaciones públicas sobre el delito como una forma de daño psíquico adicional para las víctimas, daño que evidentemente es mayor si se ven expuestas a conductas humillantes. La alusión a los familiares sería coherente con esta interpretación en la medida que sean concebidos como víctimas indirectas.

La reforma de 2015 ha previsto una nueva cualificación (artículo 578-2) cuando las conductas se lleven a cabo a través de medios de comunicación, internet, comunicaciones electrónicas o uso de tecnologías de la información y la comunicación. También ha incluido en el número 4 una serie de medidas encaminadas a evitar el carácter permanente de la ofensa que deriva de su comunicación en línea, mediante la destrucción, el borrado o inutilización de los archivos o soportes, así como la retirada de los contenidos cuando el delito se hubiera cometido a través de las TIC. García Albero (2016) ha criticado la confusión y contradicción que supone que, en principio, se prevea la retirada de contenidos con carácter preceptivo y después, en el párrafo segundo, la medida resulte facultativa. El embrollo lo resuelve el autor interpretando que la medida es facultativa para el tribunal sentenciador solo en lo que afecta a las órdenes de retirada del servicio, a la supresión de enlace y al bloqueo de acceso, mientras que la mera retirada de contenidos es preceptiva.

## 5. Análisis de jurisprudencia

A continuación, se exponen los resultados de una evaluación de la respuesta judicial a la dinámica expansiva de los delitos de odio cometidos mediante las redes sociales. Una observación del número de sentencias muestra con claridad un incremento de la actividad jurisdiccional, de lo que es muestra el número de casos que ha llegado al Tribunal Supremo. El estudio aporta información dirigida a verificar hasta qué punto pueden tener relevancia para explicar la respuesta judicial las siguientes hipótesis: a) el incremento de los delitos de odio, propiciado por el uso masivo de las redes sociales; b) el aumento de la sensibilidad social respecto a estos delitos; c) el incremento de su persecución derivado básicamente de la actividad de las policías y la Fiscalía; d) una actitud más punitiva respecto a determinadas formas de expresión de ciertos sectores sociales o individuos que canalizan su rabia, disconformidad y protesta social mediante una presencia hostil en las redes sociales.

Para ello, se han analizado todas las sentencias dictadas por el TS entre 1 de enero de 2015 y 28 de febrero de 2018. Una vez excluidas las correspondientes a delitos distintos a los de los artículos 510 y 578, han resultado dieciocho sentencias. La evolución de las resoluciones es indicativa del proceso expansivo: dos corresponden a 2015, tres a 2016, nueve a 2017 y cuatro al período de tan solo dos

meses de 2018. A ello se añade que prácticamente no hay sentencias anteriores a 2015.

La revisión de las sentencias (ver tabla 1) revela que la actividad de los tribunales se ha centrado básicamente en el delito de enaltecimiento del terrorismo, siendo residuales los supuestos de provocación al odio con aplicación del artículo 510 que han llegado al más alto tribunal. Los medios de comunicación empleados han sido fundamentalmente Twitter y Facebook, y en menor medida otras redes sociales. La mayor parte de sentencias hacen referencia a autores de perfil ideológico izquierdista que difundieron elogios a ETA y al GRAPO. También se han emitido condenas relacionadas con la apología del terrorismo de base islamista y una por provocación al odio de género desde una ideología machista. La mayoría de sentencias han confirmado las resoluciones previas de la Audiencia Nacional y la mayoría de pronunciamientos han sido condenatorios, con presencia de algunos votos particulares que expresan una posición liberal minoritaria en el seno del Tribunal. Las penas impuestas por el delito del artículo 578 oscilan entre un año y dos años de prisión (por lo tanto, en la mitad inferior del marco penal legal), más inhabilitación absoluta, salvo los supuestos en que se ha aplicado una pena inferior por la existencia de alguna atenuante. El único caso en que se ha aplicado el artículo 510 se ha impuesto una pena más grave, de dos años y seis meses de prisión y multa.

Un análisis basado en la fundamentación jurídica de las sentencias confirma la consolidación de una línea jurisprudencial que interpreta los delitos de odio, particularmente el tipo delictivo del artículo 578, a partir de una concepción restrictiva de la libertad de expresión, de modo coherente con la doctrina del TC. Así, por ejemplo, en la STS 4/2017, de 11 de enero, se condenó a un cantante y letrista de rap-metal, autor además de novelas y director de cine, que había publicado diversos comentarios en una cuenta de Twitter con 8.000 seguidores, con referencias a ETA y al GRAPO y alusiones a que habría que regalar un roscón-bomba al Rey para su cumpleaños. La AN absolvió al acusado, haciéndose constar en los hechos probados que no se acreditó que el acusado con estos mensajes buscara defender los postulados de una organización terrorista, ni tampoco despreciar o humillar a sus víctimas. El TS estimó el recurso del fiscal y condenó al acusado a un año de prisión más inhabilitación absoluta. El Tribunal afirma que no todo mensaje de odio debe merecer respuesta penal, puesto que el derecho penal no puede

prohibir al ciudadano que odia ni penetrar en el ámbito de la «ética del discurso», pero rechaza que el acusado se excuse en un pretendido «nihilismo surrealista» y concluye que afirmaciones como las vertidas en la red «alimentan el discurso del odio, legitiman el terrorismo como forma de solución de los conflictos sociales y, lo que es más importante, obligan a la víctima al recuerdo de la lacerante vivencia de la amenaza, el secuestro o el asesinato de un familiar cercano». Todo ello a partir de los precedentes de sentencias previas y de la doctrina constitucional fijada en la STC 112/2016, tras recordar que el tipo subjetivo del delito objeto de examen no exige más que el dolo y subrayar la intensificación del daño que deriva de la utilización de las TIC, por el efecto de perpetuidad y la imposibilidad de control sobre los contenidos difundidos en la red.

La citada STS cuenta con un voto particular de Perfecto Andrés Ibáñez, quien afirma que las frases recogidas en los hechos probados son fielmente expresivas de la subcultura de algunos grupos sociales, integrados por jóvenes que contestan la cultura de un establishment del que, no sin razón, se consideran excluidos. Según el magistrado, sus expresiones son un modo de provocar o escandalizar, sin que pueda considerarse que lleguen a «justificar» el terrorismo, algo que reclamaría «un discurso mínimamente articulado», ni tengan «la menor posibilidad de conexión práctica con algún tipo de actores y de acciones» de carácter terrorista. El voto particular se inscribe así en la interpretación restrictiva que exige que la emisión del mensaje de odio entrañe un riesgo de comisión efectiva de delitos de terrorismo.

Otra muestra del criterio predominante en el TS es la Sentencia 706/2017, de 27 de octubre, que confirmó la condena a un usuario de Twitter que había retuiteado un vídeo y diversos mensajes con textos e imágenes de apoyo a ETA. Esta resolución retorna a la línea jurisprudencial restrictiva respecto a la libertad de expresión, tras anteriores pronunciamientos de signo absolutorio, como la STS 378/2017, de 25 de mayo. Esta sentencia fue consecuente con lo previsto en la Directiva UE/2017/541, cuyo artículo 5 acota la penalización de la provocación al terrorismo a los casos en que «se preconice directa o indirectamente, a través, por ejemplo, de la apología de actos terroristas, la comisión de delitos de terrorismo, generando con ello un riesgo de que se puedan cometer uno o varios de dichos delitos». Sin embargo, en la STS 706/2017 se renunció al potencial restrictivo derivado de esa concepción que



vincula el delito al riesgo. El acusado colgó y retuiteó en abierto en su cuenta de Twitter, seguida por 120 usuarios, materiales ajenos que ya circulaban por internet, con siglas de ETA y del IRA, imágenes de encapuchados y del funeral de cuatro terroristas, lemas alusivos a la Kale Borroka o la expresión «Adiós con honor» referida a algunos terroristas. La desvinculación entre estos hechos y el riesgo de comisión de delitos es patente dado que el Tribunal no realiza ninguna alusión al riesgo como criterio de restricción del ámbito de lo típico y, además, los mensajes se difundieron cuatro años después de haber cesado ETA su actividad violenta. Asimismo, el Tribunal considera irrelevante que los mensajes hubieran sido meramente retuiteados y niega todo carácter limitador a la dimensión subjetiva de la conducta del autor. La sentencia ha recibido críticas (Cabellos Espiérrez 2017).<sup>12</sup>

Fuera ya del ámbito del artículo 578 CPE y del contexto de la apología del terrorismo, el TS, en la Sentencia 72/2018, de 9 de febrero, relativa a un caso de discriminación de género, señaló que «el discurso del odio es claro en su afirmación antijurídica y típica, en la medida en que el autor vierte las expresiones contra las mujeres, y particularmente, respecto de las que han sido objeto de una vejación y un maltrato físico». En uno de sus tuits, el acusado afirmó: «53 asesinadas por violencia de género machista en lo que va de año, pocas me parecen con la de putas que hay sueltas». En otro: «Y 2015 finalizará con 56 asesinadas, no es una buena marca pero se hizo lo que se pudo, a ver si en 2016 doblamos esa cifra, gracias». En otra cuenta de Twitter aludió a una mujer asesinada cuyo cadáver fue echado al río por su asesino indicando que «era feminista y se tiró al río porque las mujeres se mojan por la igualdad». En la misma sentencia el TS revocó la condena por enaltecimiento del terrorismo que le había impuesto la AN, al ser las expresiones utilizadas por el acusado muy genéricas y carentes de peligrosidad.

Posteriormente, en la STS de 15 de febrero de 2018 se condenó a un rapero por difundir a través de YouTube

canciones que incluyen expresiones en apoyo de ETA y los GRAPO, además de injurias al Rey y sus familiares y amenazas contra otra persona. El acusado alegó haber actuado en ejercicio del derecho a la libertad de expresión y a la creación artística, dado que «el lenguaje del rap es extremo, provocador, alegórico y simbólico», pero el Tribunal entendió que una lectura de los hechos es suficiente «para comprender la gravedad de las expresiones contenidas y su correcto encaje en los tipos penales de referencia». Sin embargo, casi al mismo tiempo, en la STS 95/2018, de 26 de febrero, se absolvió a la acusada de un delito de enaltecimiento del terrorismo por el que había sido condenada por la AN, por haber difundido a través de Twitter chistes sobre Carrero Blanco, con el argumento de que ello implicaba penalizar meros chistes de mal gusto referidos a una persona muerta hacía ya cuarenta años.

En el futuro inmediato, cabe esperar que la actividad judicial respecto a estos delitos siga viva. Muestra de ello son, por una parte, los diversos procedimientos abiertos por mensajes difundidos en el contexto del conflicto político derivado del proceso secesionista catalán. Por otra parte, siguen apareciendo sentencias de la Audiencia Nacional, como la 34/2017, de 4 de diciembre, la 1/2018, de 22 de enero, y la 3/2018, de 2 de marzo, las tres con un voto particular favorable a un fallo absolutorio.<sup>13</sup> En la primera de ellas, se condenó a dos años de cárcel por delito de enaltecimiento del terrorismo a cada uno de los doce músicos que de un grupo de hip-hop que difundieron mensajes apologéticos respecto a los GRAPO a través de un canal de YouTube con 3.400 seguidores, al concluir que de forma unitaria buscaban propagar sus ideas de odio al sistema democrático y ensalzar la mencionada organización terrorista.<sup>14</sup> La presidenta de la Sección, en su voto particular, minimizó la trascendencia del comportamiento de los jóvenes, entendiendo que tan solo querían llamar la atención, «sin una intencionalidad dirigida a enaltecer o justificar acciones terroristas». En la segunda sentencia citada, la Audiencia condenó a medio año de cárcel a un tuitero por publicar en su cuenta personal frases de

12. El autor ha lamentado la ausencia de criterios claros en la práctica judicial: «La vaguedad del artículo 578 CP parece haberse trasladado y multiplicado en su paso a la aplicación judicial, y la predictibilidad de las resoluciones judiciales es, en este punto, ciertamente mejorable».
13. Hay que destacar sin embargo la SAN3/2018, de 2 de febrero, por enaltecimiento del terrorismo, de signo absolutorio.
14. Los doce condenados hicieron públicas proclamas a favor de la libertad de los presos políticos y del «Partido Comunista Reconstruido», así como elogios a diversos miembros de los GRAPO. Entre otras frases, afirmaron: «Pero como esto siga así y no encuentre alternativa, atracaré bancos, los responsables saborearán la cal viva, si es que no llegan tan arriba como Carrero Blanco».

deshonra y burla referidas a víctimas de ETA.<sup>15</sup> El Tribunal apreció que el acusado mostró arrepentimiento y «real aflicción» por los hechos, lo cual le valió una atenuación de la pena, pero no un fallo absolutorio, al considerar que la emisión de tal clase de expresiones no queda amparada por la libertad de expresión. El Tribunal considera que ello va más allá del mal gusto y no puede atribuirse a una ofuscación o a una reacción impulsiva, dada la reiteración de la conducta ofensiva durante tres años. En la tercera, se condenó a un rapero por enaltecimiento del terrorismo e injurias al Rey, con la agravante de reincidencia, a una pena de dos años y un día de prisión. El acusado no ha mostrado arrepentimiento y ha reproducido los mismos mensajes que le valieron la condena.<sup>16</sup>

La posición predominante en la AN ha recibido críticas doctrinales. Así, Correcher Mira (2017) ha reprochado la

respuesta punitiva de este tribunal ante «la expresión en las redes de opiniones políticas, humor negro o cualquier otra manifestación que pueda considerarse ofensiva según qué estándares morales». Según el autor, esta tendencia «supone una criminalización en las redes sociales de opiniones que nada tienen que ver con la actividad terrorista, sino que representan una posición de disenso respecto del pensamiento político y cultural hegemónico». La propia Fiscalía General del Estado ha puesto de manifiesto las contradicciones existentes entre las sentencias de la Audiencia, advirtiendo que no puede equipararse al enaltecimiento del terrorismo hechos como reenviar un chiste de mal gusto.<sup>17</sup> Pese a que es obvia la existencia de visiones y sensibilidades distintas en el interior de la judicatura, la posición de la Audiencia tiene de momento el respaldo del criterio mayoritario entre los magistrados del TS.

Tabla 1. sentencias del Tribunal Supremo por delitos de odio a través de redes sociales

Fecha resolución	Artículo CP	Contexto <sup>18</sup>	Red social	Seguidores	Sentido fallo	Pronunciamiento	Penas	Votos particulares
19-02-15	578	ETA, Grapo Al Qaeda y otros	YouTube	Abierto	Desest.	Condena	Prisión 24 m + inhab.	no
30-12-15	578	Estado Islámico	Facebook	Muro abierto	Desest.	Condena	Prisión 26 m + inhab.	no
13-07-16	578	ETA	Facebook	Abierto	Est. parcial	Condena	Prisión 12 m + inhab.	no
02-11-16	578	ETA	Twitter/ Facebook	5.577 / 1.238	Desest.	Condena	Prisión 18 m + inhab.	no
15-12-16	578	ETA, Grapo	Facebook	Abierto	Desest.	Condena	Prisión 12 m + inhab.	no
18-01-17	578	ETA, Grapo	Twitter	8.000	Desest.	Condena	Prisión 18 m + inhab.	1: absol.
28-03-17	578	ETA	Twitter	Abierto	Estim. parcial	Condena art. 21-1 / 20-1 CP	Prisión 6 m + inhab.	no

15. Algunas de las frases publicadas en Twitter fueron: «A tomar culo y Gora ETA» o «Faltan tiros en la nuca», señalando a víctimas asesinadas por ETA con su nombre y diciendo que «tiene un agujero en el cogote como los delfines», o en relación a una víctima que había resultado mutilada en un atentado escribió que «ha salido por patas».
16. El acusado había sido ya condenado por la Audiencia Nacional en 2014. La sentencia de 2018 tiene un voto particular de Manuela Fernández Prado, que sostiene que los hechos imputados quedan bajo la cobertura de la libertad de expresión.
17. Así, Memoria FGE 2017, pág. 743-744.
18. Organización terrorista respecto a cuyas acciones se expresa la apología o justificación o bien otros elementos indicativos del contexto.

Fecha resolució	Artículo CP	Contexto <sup>18</sup>	Red social	Seguidores	Sentido fallo	Pronuncia-miento	Penas	Votos particulares
05-07-17	577-2	Estado Islámico	Facebook, Twitter, Tuenti, YouTube (42 perfiles)	Abierto	Desest.	Condena	Prisión 7 años	no
11-05-17	578	ETA	Twitter	Abierto 406	Estim. parcial	Condena art. 20-7 / 21-1 / 20-1	Prisión 9 m + inhab.	2: eximente 20-1
25-05-17	578	Grapo, ETA	Facebook		Estim.	Absolución		no
13-07-17	578	Estado Islámico	Facebook	Abierto	Desest.	Absolución		no
25-07-17	578	ETA	Twitter	Abierto	Desest.	Absolución		no
05-10-17	577-2	Estado Islámico	Facebook	Abierto	Desest.	Condena	Prisión 8 años + multa retirada internet	no
27-10-17	578	ETA	Twitter	Libre acceso 121	Desest.	Condena	Prisión 18 m + inhab.	no
31-01-18	578	ETA	Twitter	Abierto	Desest.	Absolución		no
09-02-18	510 / 578	Apología de la violencia de género	Twitter	2.000	Est. parcial	Condena 510 absolución 578	Prisión 30 m y multa	no
15-02-18	578	Injurias al rey y amenazas	YouTube	Abierto	Desest.	Condena	Prisión 24 m + inhab.	no
26-02-18	578	ETA	Twitter	4.478	Estim.	Absolución		no

Fuente: Elaboración propia

## 6. Conclusiones y propuestas

El análisis efectuado ha revelado que la actividad de los tribunales en España ha respondido al incremento del uso de las redes sociales y a la introducción en las mismas de elementos propios del discurso del odio, sin olvidar la actividad desarrollada por las policías y la Fiscalía contra algunas manifestaciones de este discurso. Al mismo tiempo, se ha evidenciado que el porcentaje de casos enjuiciados, en comparación con el número de denuncias y procedimientos iniciados, es bajo y centrado principalmente en el delito de enaltecimiento del terrorismo y humillación a sus víctimas. Pese a la existencia de criterios diversos entre los jueces, que se refleja en algunos vaivenes y votos particulares, se imponen las tesis más punitivas y restrictivas respecto a la libertad de expresión ante manifestaciones caracterizadas por un lenguaje provocador y alejado de los cánones de la elegancia y la corrección política, como medio de expresión

de la rabia y la frustración existente en cierto sector de la juventud. Ante este panorama, los juzgadores deberían recordar que el derecho a la libertad de expresión comprende también el derecho a expresarse de modo inadecuado, incómodo e incluso hostil o hiriente para muchos, y que el límite entre el discurso del odio reprobable y el odio penalmente relevante debería estar en el riesgo que su exteriorización puede entrañar de comisión de hechos delictivos, según la cláusula de idoneidad que deriva de la Directiva europea de 2017. Asimismo, el legislador debería tener en cuenta que un adecuado respeto al principio de proporcionalidad requiere reservar la pena de prisión a los supuestos en que el mensaje de odio se exprese por medios violentos, mediante una razonable concepción gradual de la respuesta punitiva. El programa penal ilustrado del CP de 1995, que suprimió el delito de desacato, redujo la apología a los supuestos de provocación al delito y eliminó las penas de prisión para los delitos de injuria o ultrajes a la nación,

ha sido desbaratado mediante la incriminación del enaltecimiento del terrorismo, un uso perverso del argumento del discurso del odio o una aplicación inversa o inmoderada del artículo 510. En manos de un buen legislador está revertir esta dinámica, situando en su sitio adecuado los delitos de odio contra colectivos socialmente vulnerables y confiando a los programas de prevención extrapenales,

tecnológicos o educativos (García González, 2015) la respuesta al discurso del odio y la protección de los menores frente a los riesgos de las TIC y las redes sociales. Y en manos de los jueces está revertir la tendencia jurisprudencial hasta ahora dominante, adoptando la doctrina de la Corte Europea de Derechos Humanos que ha situado en su lugar adecuado la respuesta ante el discurso del odio.

## Referencias bibliográficas

- AGUSTINA SANLLEHÍ, J. R. (2014). «Victimología y victimodogmática en el uso de las TIC». En: TAMARIT, PEREDA (coord.). «La victimología ante las nuevas formas de victimización». Buenos Aires-Madrid-Montevideo: ed. Bdf/Edisofer.
- ALCACER GUIRAO, R. (2012). «Discurso del odio y discurso político. En defensa de la libertad de los intolerantes». *Revista electrónica de ciencia penal y criminología*.
- ALCÁCER GUIRAO, R. (2016). «Diversidad cultural, intolerancia y Derecho penal». *Revista electrónica de ciencia penal y criminología*, 18-11.
- ALCÁCER GUIRAO, R. (2018). «Opiniones constitucionales». *InDret*, 1/2018.
- ALONSO RIMO, A. (2010). «Apología, enaltecimiento del terrorismo y principios penales». *Revista de Derecho penal y Criminología*, v. 4.
- CABELLOS ESPIÉRREZ, M. A. (2017). «Retuitear es delito? A propósito de la STS 2017». *Revista de Dret públic de Catalunya - Blog*: 13.12.2017.
- CKAKRABORTI, N.; GARLAND J. (2012). «Reconceptualizing hate crime victimization through the lens of vulnerability and difference». *Theoretical Criminology*, n.º 16(4), 2012, p. 499-514. <<https://doi.org/10.1177/1362480612439432>>
- CORRECHER MIRA, J. (2017). «El delito de enaltecimiento del terrorismo y humillación a las víctimas tras la reforma de la LO 2/2015 en materia de delitos de terrorismo». *Revista General de Derecho penal*, n.º 27.
- FUENTES OSORIO, J. L. (2017). «El delito como odio». *Revista electrónica de ciencia penal y criminología*.
- GARCÍA ALBERO, R. (2016). «Comentario al artículo 578». En: G. QUINTERO OLIVARES (dir.). *Comentarios al Código penal español*, 7ª ed., Pamplona: ed. Aranzadi.
- GARCÍA GONZÁLEZ, J. (2015). «Oportunidad criminal, Internet y redes sociales». *InDret*, 4/2015, pág. 1-32.
- GARLAND, J. (2011). «Difficulties in defining hate crime victimization». *International Review of Victimology*, vol. 18, no. 1, pág. 25-37. <<https://doi.org/10.1177/0269758011422473>>
- GÓMEZ MARTÍN, V. (2012). «Discurso del odio y principio del hecho». En: MIR PUIG y CORCOY BIDASOLO (dir.). *Protección penal de la libertad de expresión e información. Una interpretación constitucional*. Valencia: ed. Tirant lo Blanch.
- IGANSKI, P.; LAGOU, S. (2015). «Hate crimes hurt some more than others: implications for the just sentencing of offenders». *Journal of Interpersonal Violence*, v. 30 (10), pág. 1696-1718. <<https://doi.org/10.1177/0886260514548584>>
- KARMEN, A. (2013). «Crime victims. An introduction to victimology». 8ª ed, Belmont.
- LANDA GOROSTIZA, J. M. (1999). *La intervención penal frente a la xenofobia*. Bilbao: ed. Universidad del País Vasco.

- LANDA GOROSTIZA, J. M. (2001). *La política criminal contra la xenofobia y las tendencias expansionistas del Derecho penal*. Granada: ed. Comares.
- MASON, G. (2014). «The symbolic purpose of hate crime law: Ideal victims and emotion». *Theoretical Criminology*, vol. 18, no. 1, pp. 75-92. <<https://doi.org/10.1177/1362480613499792>>
- MIRO LINARES, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología* (13).
- MIRÓ LINARES, F. (2015). «La criminalización de conductas 'ofensivas': A propósito del debate anglosajón sobre los 'límites morales' al Derecho penal». *Revista electrónica de ciencia penal y criminología*.
- PERRY, B. (2009). *Hate crimes: responding to hate crime*. Ed. Praeger publishers.
- PORTILLA CONTRERAS, G. (2015). «La represión penal del discurso del odio». En: G. QUINTERO OLIVARES, *Comentario a la reforma penal de 2015*. Pamplona: ed. Aranzadi.
- TAMARIT SUMALLA, J. (2013). «Paradojas y patologías de la construcción social, jurídica y política de la victimidad». *InDret*.
- TAMARIT SUMALLA, J. (2018). «¿Las interacciones sexuales en línea son abuso sexual? Peculiaridades de la victimización sexual de menores a través de las TIC». *Revista IDP*, n.º 26, pág. 30-42.

### Cita recomendada

TAMARIT SUMALLA, Josep M. (2018). «Los delitos de odio en las redes sociales». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 17-29. UOC [Fecha de consulta: dd/mm/aa]  
 <<http://dx.doi.org/10.7238/idp.v0i27.3151>>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre el autor

Josep M. Tamarit Sumalla  
 jtamarit@uoc.edu

Catedrático de Derecho penal (UOC)

<<https://www.uoc.edu/portal/es/news/kit-premsa/guia-experts/directori/josepm-tamarit.html>>

UOC

Av. Carl Friedrich Gauss, 5  
 08860 Castelldefels



**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## ARTÍCULO

# Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)

Carmen Tomás-Valiente Lanuza

Universitat de les Illes Balears

Fecha de presentación: mayo de 2018

Fecha de aceptación: julio de 2018

Fecha de publicación: septiembre de 2018

## Resumen

Las redes sociales constituyen vehículos de exhibición de la propia intimidad a la vez que canales especialmente idóneos para la exposición de la ajena. En esta última variante, en los últimos años han devenido en medio comisivo preferente de delitos de revelación de secretos del artículo 197 Cp en sus distintas modalidades (el encaje en una u otra dependerá del modo en que se haya accedido al material íntimo objeto de la difusión); el usuario de la red es aquí el autor del delito contra la intimidad ajena (apartado 1). De otro lado, en cambio, el usuario de una red social se coloca también a sí mismo en una posición vulnerable (apartado 2), puesto que aquello que publica a un círculo cerrado de destinatarios (los «amigos»), que eventualmente puede afectar a su intimidad, es susceptible de ser redifundido por alguno de estos, conducta que, pese a todo, no consideramos penalmente típica. En tercer lugar, la jurisprudencia más reciente empieza a ocuparse de supuestos de acceso no consentido al espacio de un usuario en una red social (apartado 3), en los que entra en juego la figura de intrusismo informático del artículo 197 bis.

## Palabras clave

red social, intimidad, descubrimiento y revelación de secretos, intrusismo informático

## Tema

protección penal de la intimidad



## Privacy offences and social networks (particularly in the most recent case-law)

### Abstract

Social networks constitute new windows for displaying one's own private life, while also being particularly suitable channels for exposing the privacy of others. In this last sense, they have recently become a most frequent vehicle for the crime of disclosing secrets, contained in Article 197 of the criminal code in its different forms (the conduct's specific classification among them depends on how the shared intimate material was obtained). Here, the user of the network is the perpetrator of the privacy offence (section 1). On the other hand, social network users also place themselves in a vulnerable position (section 2), since everything they intend to show to a closed circle of recipients (their "friends"), which may eventually affect their privacy, can afterwards be passed on by any of these people—a conduct which, despite everything, we do not consider criminal. Thirdly, the most recent case-law has begun to deal with cases of non-consensual access to a user's space in a social network (section 3), where article 197 bis crime of computer hacking comes into play.

### Keywords

social network, privacy, discovery and revealing of secrets, computer hacking

### Topic

criminal protection of intimacy

## Introducción

El uso masivo de las redes sociales (especialmente de las denominadas «de ocio») ha modificado de modo muy relevante -afirmarlo constituye ya un lugar común- la manera de entablar y mantener relaciones interpersonales, en un nuevo escenario en el que -entre otros muchos factores- resulta fundamental la transformación del papel desempeñado por la intimidad de los usuarios. Las redes sociales sirven, ante todo, como canal de exposición o comunicación (en abierto o a círculos más o menos restringidos de destinatarios) de la propia intimidad (fotos, vídeos, información sobre gustos, actividades, etc.), aunque obviamente también operan como vehículo de difusión de lo que puede afectar a la intimidad de terceros no usuarios que no hayan prestado su consentimiento a dicha exposición.<sup>1</sup>

En estas páginas intentaremos diseccionar (o cuando menos sistematizar), sobre la base de la jurisprudencia más

reciente, las cuestiones jurídico-penales específicamente suscitadas por la utilización de una red social en la comisión de hechos eventualmente incardinables en los delitos de descubrimiento y revelación de secretos (artículo 197), aunque también se planteará la aplicabilidad del delito de intrusismo informático del artículo 197 bis Cp a supuestos en los que la red social opera no como instrumento de la comisión del delito, sino como objeto material mismo de la conducta (como sucede en los casos de acceso no consentido a la página de un usuario).

### 1. La red social como vehículo de difusión de la intimidad de terceros distintos del usuario

Dejando en este momento al margen las peculiaridades de la protección de la libertad informática o *habeas data*

1. Una interesante introducción al fenómeno de las redes sociales, en tanto nuevo marco de hechos penalmente relevantes contra diversos bienes jurídicos (intimidad, inviolabilidad informática, honor, propiedad intelectual, etc.) con los usuarios como posibles autores y víctimas, puede encontrarse en Picotti (2013, pág. 76-81).

por el artículo 197.2, la tutela penal de la intimidad por el artículo 197 se articula básicamente, como es sabido, en torno al modo de acceso (ilícito o lícito) a aquello en lo que se plasma la intimidad (documentos, cartas, mensajes, fotografías, vídeos...). Hasta la reforma del precepto por la LO 1/2015, nuestro ordenamiento solo sancionaba el acceso ilícito (descubrimiento) y la eventual revelación de lo así conocido.<sup>2</sup> A partir de la citada reforma, la revelación de lo ilícitamente conocido conserva un mayor reproche penal, pero también es típica, en los términos que enseguida se comentarán, la difusión (siempre no consentida) de imágenes o grabaciones de contenido íntimo previamente obtenidas con consentimiento del sujeto pasivo (se tipifica por tanto, y con una pena menor que la variante anterior, la revelación de lo que el autor ha conocido lícitamente).

### 1.1. Revelación o difusión de aquello a lo que se ha accedido ilícitamente (artículos 197.1 y 197.3 Cp)

#### 1.1.1. Los accesos ilegítimos típicos (del artículo 197.1) previos a la difusión.

El ámbito tradicional de protección penal del bien jurídico (el único típico antes de 2015) viene dado por el acceso ilegítimo a la intimidad, en cualquiera de las modalidades descritas por el prolijo apartado 1 (apoderarse de documentos, mensajes, fotos, etc.; interceptar las comunicaciones; o utilizar de artificios técnicos de escucha o grabación del sonido o de la imagen), a partir de lo cual la conducta puede detenerse en ese mero descubrimiento de la intimidad ajena (al que dicho apartado asigna una pena de uno a cuatro años de prisión más multa) o avanzar hasta la ul-

terior revelación de lo descubierto a terceras personas (lo que da lugar al tipo agravado del apartado 3, con pena de dos a cinco años). En relación con esta segunda conducta, en la práctica las redes sociales, junto con la mensajería telefónica (sobre todo a través de la aplicación WhatsApp), juegan un papel destacado como canales de revelación o difusión, lo que normalmente comporta un grado de lesividad más intenso (en función del número de personas con acceso al perfil del usuario) que en las revelaciones dirigidas a un número menor de destinatarios.

En todo lo que se refiere a la satisfacción de los requisitos típicos del artículo 197.1, sobre los que se construye la posterior conducta de revelación, la intervención de la red social como instrumento de esta última no introduce, como es lógico, ninguna diferencia. Es necesario que antes de la revelación o difusión se haya producido alguna de las conductas invasoras de la intimidad del citado apartado, cuyos requisitos típicos han de haberse cumplido en su totalidad (con los problemas interpretativos a que pueden dar lugar, por ejemplo, el concepto de apoderamiento,<sup>3</sup> o la determinación de aquello que puede entenderse que afecta a la intimidad).<sup>4</sup> Todo ello se satisface, sin duda, en los supuestos que la jurisprudencia nos demuestra más frecuentes en la práctica, aquellos en los que se difunden fotografías o vídeos de carácter sexual obtenidos sin consentimiento de la persona que en ellos aparece, y que obran en poder del autor de la difusión bien porque previamente se ha «apoderado» de ellos (así, si entra sin autorización en el correo electrónico de la víctima o en su teléfono móvil, y se descarga las imágenes que allí encuentra),<sup>5</sup> bien porque él mismo ha utilizado artificios de captación de imágenes

2. Salvo en el caso de la revelación de secretos conocidos por razón del oficio o profesión (artículo 199), cuyo presupuesto es siempre el acceso lícito a la información.
3. ¿Constituye apoderamiento la mera lectura de lo que otro ha dejado -con mayor o menor grado de descuido- a la vista de terceros? ¿Y fotografiarlo? De este último supuesto, afirmando la tipicidad, se ocupa la SAP Ciudad Real 180/2017, de 30 de noviembre. De todos es conocido, por otra parte, el reciente suceso de la captación con cámaras de televisión (y posterior difusión) de mensajes privados intercambiados entre dos políticos catalanes, que aparecían en la pantalla del teléfono móvil de uno de ellos, a la vista del equipo periodístico.
4. Así, la captación de fotografías en plena calle de dos personas besándose, realizada sin consentimiento de los fotografiados, no encaja en el apartado 1 (ni su posterior revelación, por tanto, en el apartado 3) por mucho que aquello que evidencien (en el supuesto de la SAP Jaén 76/2017, de 31 de enero, una relación extramatrimonial) sí pueda formar parte de la intimidad del fotografiado. Conductas de este tipo (captación y difusión de imágenes que no pueda decirse que afecten a la intimidad, teniendo en cuenta el lugar en el que se toman y su propio contenido) han de remitirse necesariamente a la protección civil de la propia imagen. Absuelve por ello acertadamente la SAP Madrid 539/2017, de 26 de junio, a quien graba en la calle y difunde luego en su Facebook un vídeo de un niño de dos años cuando, acompañado por su padre, tiene una fuerte rabieta.
5. SAP Málaga 396/2015, de 9 de septiembre. Aunque la sentencia no entre en ello en absoluto, los hechos suscitan un viejo problema de tipicidad del artículo 197.1, que se produce cuando el autor se apodera ilícitamente de material íntimo (en este caso, fotos que se descarga del móvil de su expareja), pero dándose la circunstancia de que la persona cuya intimidad se refleja no es la «dueña» del material (en este supuesto, quien aparece en las fotos no es el dueño del móvil, sino su nueva pareja, desnuda). Se suscita entonces la duda de si se



de la víctima de modo subrepticio<sup>6</sup> (o advertido pero no consentido, como cuando se graba una agresión, que no necesariamente tiene que serlo contra la libertad sexual).<sup>7</sup>

#### 1.1.2. La difusión en cadena a través de las redes

En este contexto, la peculiaridad planteada por el uso de redes sociales como instrumento de revelación del material íntimo se refiere a la conducta de redifusión o reenvío, cuando es realizada por quienes no han intervenido en su ilícita obtención; conducta que, siempre que el sujeto conozca dicho origen ilícito, es sancionada por el artículo 197.3 párrafo segundo con la pena de uno a tres años de prisión más multa. Pues bien, en principio, en la medida en que cada sujeto que comparte el material en sus redes sociales amplía sucesivamente el círculo de conocedores, con cada redifusión se produce una nueva lesión del bien jurídico protegido, cuya relevancia penal a la luz del precepto mencionado no plantea problemas.<sup>8</sup>

#### 1.1.3. El indebido recurso al artículo 197.2 Cp para soslayar la atipicidad del acceso previo a la difusión

Una vez sentada la necesidad de un acceso ilegítimo al material íntimo –típica del artículo 197.1– para poder luego sancionar ex artículo 197.3 su descubrimiento o revelación (en las redes o de cualquier otro modo), lo que no resulta de recibo es pretender soslayar los problemas de encaje en el artículo 197.1 por la vía (empleada con frecuencia creciente por las audiencias provinciales) de subsumir la conducta en el apartado 2 del artículo 197, en el que se consagra la protección penal de la llamada libertad informática o *habeas data*.<sup>9</sup> La cuestión requiere un examen algo más detenido.

La razón de ser del mencionado 197.2 (cuya atormentada redacción ha pretendido desentrañarse a través de variadas interpretaciones doctrinales) se encuentra en la protección del derecho del ciudadano a controlar sus datos personales en un contexto concreto: el de los riesgos de conocimiento y utilización no consentidos generados a partir fundamentalmente de su tratamiento informatizado. Lo que se protege son datos personales reservados (y constituye objeto de importante discrepancia cuáles de ellos puede entenderse que afectan a la intimidad merecedora de protección penal, siempre subsidiaria de la administrativa) recogidos en archivos o registros (en primera instancia, el legislador se refiere a los informatizados, aunque también admite los que no lo sean). Pues bien: siendo esto así, resulta totalmente inadecuado entender, como han propuesto diversas audiencias en los últimos años, que lo almacenado –especialmente relevante en la práctica, las fotografías o vídeos– en un dispositivo informático, como es el caso de un teléfono móvil, constituye dato *registrado* en el sentido del mencionado precepto. Adoptar esta argumentación como base para sancionar la posterior revelación de lo almacenado aboca a una ampliación potencialmente ilimitada del espacio típico del 197.2 y, a la postre, deja vacío de sentido el apartado 1: cualquier foto y cualquier documento, incluso inicialmente en papel, es susceptible de ser digitalizado y almacenado en dispositivos como móviles u ordenadores; con la argumentación que ahora discutimos, por mucho que el acceso a ellos hubiera sido lícito, su revelación sería punible por el 197.3 tomando como base el 197.2. Y lo mismo sucede (quedaría sin sentido la tipificación expresa) en relación con el nuevo apartado 7 que enseguida examinaremos.<sup>10</sup>

satisface la tipicidad en la medida en que el artículo 197.1 se refiere al apoderamiento de los papeles, documentos, etc. de una persona, realizada con ánimo de vulnerar «su» intimidad.

6. Así, SAP Madrid 671/2015, de 28 de septiembre (grabación no consentida de vídeo sexual y posterior difusión, que aquí se produce a través de páginas web de contenido pornográfico); SAP Madrid 657/2017, de 15 de noviembre (toma una foto de su novia dormida con un pecho desnudo, y tiempo después la envía a la nueva pareja de ella, además de colgarla en su Facebook). *Vid* igualmente SAP Tarragona 453/2016, de 29 de diciembre, donde la presencia o no de consentimiento resulta discutible.
7. SAP Málaga 452/2009, de 16 de septiembre.
8. No existe en España, en lo que se nos alcanza, ninguna sentencia sobre un caso de este tipo. Sí es conocido, en cambio, el supuesto sometido a enjuiciamiento en Dinamarca en el momento de escribirse estas líneas, relativo a la difusión por redes sociales de un vídeo sexual grabado sin consentimiento de sus protagonistas, y compartido sucesivamente por centenares de personas (<<http://www.lavanguardia.com/vida/20180220/44929353263/dinamarca-juicio-video-sexual-adolescentes-condenas.html>>) [Fecha de consulta: 14/0318].
9. El 197.2 impone las mismas penas que el apartado 1 al que «sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».
10. SAP Barcelona 742/2017, de 7 de septiembre, que expresamente concibe el teléfono móvil como «soporte informático donde consta un registro de archivos de carácter personal», lo que le sirve para sancionar la conducta de revelación de vídeos sexuales cuya obtención,

## 1.2. La revelación de material íntimo obtenido (lícitamente) con consentimiento del sujeto pasivo: el artículo 197.7

### 1.2.1. Conductas no abarcadas por la nueva tipificación

Como se ha comentado ya, hasta la reforma operada por la LO 1/2015, la tipicidad de las conductas de revelación se constreñía a las que tuvieran por objeto aquello previamente descubierto de modo ilícito; la revelación de lo obtenido con consentimiento de la otra persona (que en la práctica suele tener por objeto fotografías o vídeos de carácter sexual finalmente difundidos por la antigua pareja del sujeto pasivo) no encajaba en la descripción típica, por más que la difusión fuera no consentida y con independencia del innegable menoscabo, a veces muy grave, que pudiera comportar (como acontece cuando tal difusión se produce a través de una red social). La citada reforma modifica sustancialmente este panorama, si bien no con el

alcance, a mi juicio, que gran parte de la doctrina parece atribuirle.<sup>11</sup> En efecto: como ya he tenido oportunidad de poner de manifiesto en otro lugar,<sup>12</sup> la dicción del nuevo apartado 7 del artículo 197 comprende la difusión de lo que el *propio autor de la difusión* ha obtenido previamente (al grabar o fotografiar por sí mismo al sujeto pasivo), pero a mi juicio no abarca los supuestos en que las imágenes han sido obtenidas por la víctima (que se graba o fotografía a sí misma) para luego facilitarlas a quien ulteriormente las difunde sin su consentimiento. Asiste sin duda toda la razón a quienes señalan que no era esta la intención del legislador, que pretendía -aun sin cuidar la redacción para conseguirlo- incluir también los supuestos aquí discutidos<sup>13</sup> (que de hecho la jurisprudencia demuestra muchísimo más frecuentes que los primeros); la cuestión es, sin embargo, si una apelación a tales propósitos justifica una interpretación amplia del tipo que (a mi entender) desbordaría su tenor literal con la consiguiente vulneración del principio de legalidad.<sup>14</sup> En este mismo sentido se ha pro-

---

según la propia sentencia reconoce, no encajaba en el apartado 1; SAP Málaga 107/2016, de 23 de marzo (sobre la que volveremos *infra* al tratar la conducta de creación de perfiles falsos), que castiga por el 197.2 al sujeto que -con la finalidad de hacerla objeto de requerimientos sexuales por terceros- crea un perfil falso en una red social a nombre de su expareja e inserta, además de mensajes provocativos, una foto de ella (por lo demás no íntima sino inocua, y que el autor poseía legítimamente), que es considerada por la AP un dato de carácter personal cuya inserción en el perfil subsume bajo la conducta típica de utilización del dato en perjuicio del titular; SAP Burgos 136/2017, de 2 de mayo, que recurre al 197.2 para sancionar a un sujeto que publica en sus redes sociales algunos documentos (que poseía legítimamente como parte en el proceso) en los que figuraban «datos sensibles» (no se dice cuáles) de su expareja -pese a no haberse extraído los datos de archivo o registro alguno en el sentido del precepto, la AP considera que el acusado «utilizó dolosamente datos personales [de la querellante] divulgando en las redes sociales y sin su consentimiento los mismos y la situación de enfrentamiento familiar y personal existente con ella con la intención de causarle un perjuicio personal y social con dicha divulgación a la que terceras personas tenían un acceso libre»-. Con pocas explicaciones, también en un caso de difusión de una foto (sin que quede claro cómo se accedió a ella), SAP Burgos 189/2016, de 13 de mayo; por su parte, aunque absuelva, se plantea el 197.2 en un caso de difusión de un vídeo enviado por WhatsApp AAP Cádiz 445/2016, de 10 de noviembre. Correctamente en cambio, en el sentido aquí defendido y con un rechazo expreso de la aplicación del 197.2, SAP Lleida 389/2016, de 25 de octubre.

Vid. igualmente SAP Pontevedra 320/2017, de 12 de diciembre, que absurdamente condena por el artículo 197.2 cuando en realidad aquí sí se satisfacen los requisitos del apartado 1, al haber entrado el sujeto en mensajes enviados por su expareja desde su cuenta de Facebook. Por otro lado, obviamente nada de lo anterior es óbice para la sanción (*ex* artículo 197.3 en relación con el 197.2) de la revelación -en redes sociales o de otro modo- de lo que realmente constituyan datos personales reservados a los que se haya accedido sin autorización (pensemos, por ejemplo, en quien publica en su Facebook datos sanitarios de una o varias personas, que conozca por haber accedido sin autorización a registros informatizados de sus historias clínicas).

11. Artículo 197.7: «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella *que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros*, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona» (la cursiva es mía).
12. Me permito remitir a Tomás-Valiente Lanuza (2015, pág. 670-671).
13. Morales Prats (2016, pág. 1466-73). Lo cierto es que es difícilmente comprensible que se rechazaran las enmiendas presentadas por el Grupo Entesa pel Progrés de Catalunya y el Grupo parlamentario Socialista orientadas a la expresa inclusión en el precepto de los supuestos de envío del material íntimo por el sujeto pasivo.
14. Al margen de este aspecto muy discutible del tipo de *lege lata*, el delito plantea un interesante debate en cuanto a su justificación político-criminal, en el que aquí no puede ahondarse. Baste bosquejar la presencia de vectores contrapuestos: la indudable relajación de la autoprotección de la intimidad en la que incurre quien cede a otro imágenes íntimas se alza como argumento central entre sus

nunciado algún autor y alguna sentencia muy reciente;<sup>15</sup> pero lo cierto es que la mayoría de la doctrina opta por la interpretación amplia aquí criticada, al igual que la práctica totalidad de los tribunales que han tenido ocasión de pronunciarse al respecto, que dan por sentada (cosa que por cierto era previsible) la admisión como objeto material del delito de lo enviado por quien se graba o fotografía a sí mismo.<sup>16</sup>

Al margen de todo este debate, ha de advertirse, por otra parte, que a diferencia del artículo 197.3 segundo párrafo -que como se ha comentado prevé la (re)difusión eventualmente en cadena por terceras personas que no han intervenido en la obtención del material íntimo pero conocen su origen ilícito-, en esta sede no se contemplan ulteriores revelaciones por terceros (cuya consideración como típicas supondría, entre otras cosas, el carácter totalmente superfluo del 197.3.2.<sup>o</sup>).<sup>17</sup>

## 2. La red social como vehículo de exposición de la propia intimidad. La redifusión de lo recibido por los incluidos en la red social

Asumamos ahora, a efectos argumentativos (y porque como se ha dicho esta es claramente la interpretación más

defendida por doctrina y jurisprudencia), que el objeto típico del artículo 197.7 abarcara no solo las imágenes o vídeos obtenidos por quien posteriormente los revela o difunde, sino también los que voluntariamente le ha hecho llegar la persona cuya intimidad se ve «gravemente» afectada por la ulterior revelación. Pensemos en quien voluntariamente expone en su red social -al círculo más o menos restringido de sus «amigos»- imágenes que pueda considerarse que menoscaban su intimidad (no suele difundirse por las redes material comprometedor de uno mismo en el ámbito sexual, pero sí, por ejemplo, imágenes en fiestas, con amigos, etc., que según los casos -por ejemplo, si el protagonista aparece bebido o fumando droga- podrían llegar a afectar al bien jurídico);<sup>18</sup> y añádase a ello el que alguno de los destinatarios difunda las imágenes fuera de ese círculo al que iban inicialmente dirigidas. ¿Podría esta difusión considerarse típica del artículo 197.7?

Varios factores aconsejan una respuesta negativa. Ciertamente, el hecho de que el envío inicial se dirija a una pluralidad de destinatarios (los «amigos» en la red, o terminología similar) no impide *per se* (por más que el legislador parece estar partiendo de un destinatario individual) que cada uno de los que ulteriormente difundieran pudiera ser considerado sujeto activo del delito; sin embargo, este dato sí que incide sustancialmente en la interpretación de la afectación del bien jurídico y en el papel de los deberes de autoprotección razonablemente exigibles al usuario de una red social. En efecto: si las imágenes se difunden a

detractores -como mejor exponente de esta crítica Morales Prats (2016, pág. 1466-73)-, mientras que los partidarios de la tipificación suelen destacar la enorme entidad de la lesión del bien jurídico inherente a la conducta (máxime si, como es habitual, la difusión se produce en internet).

15. Mendo Estrella (2016, pág. 19 y sig.); González Collantes (2015, pág. 69-70); SAP Barcelona 302/2017, de 24 de abril.
16. SAP Guadalajara 111/2015, de 23 de septiembre y SAP Alicante 452/2016, de 3 de noviembre (aunque ambas absuelven por atipicidad en el momento de los hechos, anteriores a la creación del tipo); SAP Sevilla 314/2017, de 28 de junio; SSAP Valencia 488/2016, de 25 de noviembre, y 528/2017, de 7 de septiembre; SAP Valladolid 290/2017, de 6 de octubre. Sorprende que esta última sentencia condene por el artículo 197.7 a una mujer que detecta en el teléfono de su pareja fotos y vídeos sexuales de otra mujer, los cuales cuelga en Facebook y YouTube. Al margen del problema interpretativo mencionado *supra* en el texto (los vídeos fueron enviados por la propia víctima, y no «obtenidos» por quien difunde), la conducta no encajaría siquiera en la interpretación extensiva del precepto que aquí se rechaza (pues en modo alguno ha obtenido las imágenes y vídeos de modo consentido, ni siquiera como receptora del envío). Del relato de los hechos probados parece deducirse, en cambio, la existencia de un acceso ilegítimo a las imágenes (que se descarga, parece que inadvertidamente, del móvil de su pareja), si bien la tipicidad final de la conducta *ex artículo* 191.1 y 3 exigiría detenerse en el problema mencionado *supra* en nota 5 (las imágenes reflejan la intimidad de una tercera persona). En la doctrina, por todos, Morales Prats (2016, pág. 1466-73).
17. De ahí la incorrección de la SAP Las Palmas de Gran Canaria 81/2017, de 14 de marzo, que aunque absuelva por inaplicabilidad retroactiva del nuevo apartado 7, da por buena la tipicidad de la conducta de una joven que difunde unas fotos de otra menor (desnuda), que esta última había enviado a un sujeto que a su vez las había reenviado a la primera. A mi entender, el precepto no abarca ni la conducta de él (que no obtuvo las fotos por sí mismo, sino que las recibió de la víctima), ni desde luego la de la ulterior redifusora (que sería atípica incluso aunque la conducta del inicial destinatario de las fotos sí se considerara abarcada por el tipo).
18. Obsérvese que, aunque hubiera sido deseable en aras de una mayor restricción del tipo, el 197.7 no limita su objeto material a vídeos o fotos eróticos.

una pluralidad de destinatarios (y obviamente el argumento se refuerza cuanto más amplio sea el círculo de estos) se debilita la posibilidad de considerar que ulteriores difusiones (por mucho que se proyectaran fuera del círculo inicialmente consentido por el protagonista) menoscaban gravemente el bien jurídico intimidad; a ello se añade la absoluta renuncia del sujeto a desplegar unos mínimos deberes de autoprotección del bien jurídico, puesto que el envío a una pluralidad de destinatarios supone una total pérdida de control sobre el material remitido.<sup>19</sup> Resulta conveniente, por tanto, una interpretación restrictiva del precepto que abarque la tipicidad tan solo de aquellos supuestos en los que claramente pueda estimarse que la víctima (pese a la relajación de la autoprotección ínsita ya en el envío a una sola persona) desea mantener el material fuera del alcance de más sujetos.

### 3. La red social como objeto de acceso no consentido

#### 3.1. Precisiones iniciales

Procede ahora plantearse la posibilidad de que la red social se configure como el objeto mismo de un acceso no consentido -así, como ejemplo más frecuente en la prácti-

ca, el producido a la página de un usuario en redes como Facebook, Tuenti, Instagram, etc.-, conducta que interesa examinar a la luz del delito de intrusismo informático del artículo 197 bis (precepto al que la LO 1/2015 traslada, con algunas modificaciones, el delito de *hacking* previamente tipificado *ex novo* en el artículo 197.3 por la Ley de reforma 5/2010).

3.1.1. Distinción de las conductas de creación de un perfil falso Aunque resulte harto evidente, quizás no esté de más destacar, como precisión inicial, que el acceso no consentido al espacio ajeno en una red social no ha de confundirse con otra conducta muy distinta (objeto de un número creciente de sentencias) como es la de crear en la red social un perfil ficticio a nombre de otra persona a la que de algún modo se quiere perjudicar. Dependiendo de para qué se utilice dicho perfil falso, este comportamiento podrá resultar atípico<sup>20</sup> o dar lugar a algún delito: contra la intimidad del artículo 197.1 si el espacio se utiliza para difundir material íntimo obtenido de manera ilícita, o del 197.7 si el objeto difundido fueran fotos o vídeos de carácter íntimo obtenidos con consentimiento del sujeto pasivo (siempre en este caso que los hechos sean posteriores a la entrada en vigor de la reforma de 2015);<sup>21</sup> de la nueva figura de *stalking* o acoso del artículo 172.3. si (como en varios casos enjuiciados en los últimos años) se utilizara repetidamente la página y los datos de la víctima para, haciéndose pasar

19. Como acertadamente expresa el AAP Cádiz 445/2016, de 10 de noviembre, es difícil hablar de intimidad «en relación con episodios o incidencias (grabación de vídeo) que han sido aireadas, difundidas y divulgadas por quien invoca esa “confidencialidad”, pues como tal debemos entender quien lo sube a un grupo de 27 personas». La denunciante, en efecto, había remitido un vídeo con imágenes suyas en un bar (no se aclara en los hechos su contenido) a un grupo de WhatsApp de 27 personas, alguien del grupo lo remitió a terceros, y las imágenes terminaron finalmente colgadas en una página web. La sentencia parte de la consideración del vídeo como dato inicialmente comprendido por el 197.2 (proceder que se ha criticado *supra*), y concluye que las circunstancias mencionadas no permiten calificarlo de «reservado»; el marco de discusión correcto ha de ser, como se ha explicado, el apartado 7, pero en cualquier caso las consideraciones de la AP conducen a la valoración correcta sobre la inexistencia del menoscabo grave de la intimidad exigido por este último precepto.
20. De atípicos merecerían ser calificados, a mi juicio, los hechos enjuiciados en la SAP Madrid 658/2017, de 16 de octubre. Aunque finalmente absuelva por falta de pruebas, la sentencia parece sin embargo asumir una imprecisa tipicidad (como delito contra la intimidad) de la conducta, consistente en la apertura por el acusado de tres cuentas en Instagram, Facebook y Tuenti a nombre de su expareja, en las que cuelga «fotografías de su vida privada sin su consentimiento» -sin mencionarse en modo alguno que estas fueran íntimas ni cómo se habían obtenido-. La ulterior referencia a que «con la creación de dichas cuentas pudo [el acusado] obtener datos de los contactos de la denunciante (números de teléfono de sus allegados o de su agente de prensa), que le permitieron obtener información de la misma» no parece tampoco subsumible en ninguno de los tipos contra la intimidad.
21. SSAP Pamplona 189/2016, de 12 de septiembre y 155/2016, de 30 de junio (que absuelve de delito contra la intimidad al ser los hechos previos a la reforma de 2015, pero condena por delito contra la integridad moral del artículo 173). Llama la atención la ligereza de la SAP Málaga 4/2015, de 15 de enero, que en un supuesto de creación de un perfil falso con difusión de fotografías del suplantado (se insinúa que de carácter íntimo) confirma la condena por el artículo 197 sin especificar en ningún momento el apartado en el que se subsume la conducta, y además con particular insistencia en la irrelevancia del origen de las imágenes (lo importante según el tribunal es que se publica sin autorización fotografías obtenidas «sea legal o ilegalmente, sea con autorización o sin ella»), cuando precisamente tales datos son esenciales para la correcta subsunción de la difusión.

por ella, ofrecer servicios sexuales y conseguir así hacerla objeto de contactos por parte de terceros;<sup>22</sup> contra la integridad moral del artículo 173.1;<sup>23</sup> o, en fin, y en casos muy concretos, de delito de usurpación de estado civil del artículo 401 Cp.

### 3.1.2. Aplicación preferente del delito de descubrimiento (y eventualmente de revelación) de secretos del artículo 197.1 y 2 (y en su caso 3)

Centrándonos ya en la conducta de entrada no consentida en la página de un usuario de una red social, una segunda precisión que ha de quedar sentada desde el inicio es que el artículo 197 bis no puede acoger conductas que tienen ubicación preferente en el delito de descubrimiento de secretos del 197 apartados 1 y 2 (en su caso, seguidos de una revelación del apartado 3); de hecho, así opera la jurisprudencia cuando condena solo por estos tipos en casos en los que se produce una entrada no autorizada a un sistema informático que pudiera resultar típica *per se* de intrusismo (por ejemplo, un acceso -venciendo las medidas de protección- al correo electrónico de otra persona, al ordenador ajeno, a un registro o archivo informático de un banco, una empresa, la Seguridad Social, etc.), pero ello se utiliza para acceder a material íntimo o a datos personales reservados (se leen mensajes del correo o se ven fotos de carácter íntimo archivadas en el ordenador, objetos materiales del 197.1, o se realiza cualquiera de las conductas típicas sobre los datos registrados -de clientes, pacientes, etc.- en el caso del 197.2).<sup>24</sup> Por esta razón, si tenemos en cuenta que la mayoría de las redes sociales incorporan el servicio de intercambio de mensajes individuales con otro usuario, entiendo que el descubrimiento de estos por quien previamente se ha introducido sin permiso en la página debe encuadrarse directamente en el

primer apartado del artículo 197, que absorbe todo el desvalor del hecho (concurso de leyes resuelto por principio de consunción).<sup>25</sup>

Sin abandonar todavía la reflexión sobre las posibilidades de aplicar preferentemente el artículo 197.1 a la conducta de entrada no consentida en una red social, en principio parece claro que -a menos que se produjera la apertura de mensajes individualizados que acaba de mencionarse- dicha entrada no daría lugar *per se* a un delito de descubrimiento de secretos; como se ha comentado ya en apartados anteriores, parece lógico entender que lo que un usuario ha mostrado voluntariamente a otros a través de la red social (pensemos sobre todo en fotografías o vídeos, incluso aunque estas tuvieran un carácter inicialmente íntimo)<sup>26</sup> deja de pertenecer a su intimidad, al menos (entiendo) en el grado en que sería acreedora de protección penal. Es cierto que en el caso que nos ocupa quien entra en la página de la red social sin consentimiento del titular no pertenece al círculo de personas con las que este ha querido compartir su (inicial) intimidad (que son solo aquellos previamente aceptados por él como destinatarios), y en este sentido la calificación de la conducta podría ofrecer más dudas. La cuestión merecería sin duda una reflexión más detenida de la que puede acometerse en estas páginas; con todo, creo que aquello que ya se ha compartido con terceros (en un círculo que, si hablamos de redes sociales, siempre implica ya una cierta amplitud) no entraría en el círculo de la intimidad penalmente protegible. En tales casos de inaplicabilidad del artículo 197.1 sí podría plantearse ya, en cambio, la entrada en juego del intrusismo informático del 197 bis, un delito de contornos nada precisos y a día de hoy todavía muy poco aplicado por los tribunales (situación que no brinda demasiados

22. Esta, tras la entrada en vigor de la reforma, sería la ubicación apropiada para la conducta enjuiciada en la SAP Málaga 107/216, de 23 de marzo, que sin embargo condena, con el recurso argumental ya criticado *supra* en el texto, por el artículo 197.2 (al haberse incluido en el perfil falso una foto de la víctima -por lo demás inocua- que el sujeto tenía almacenada -lícitamente- en su teléfono móvil, foto que la sentencia considera dato personal).
23. Sobre la aplicabilidad de este y otros tipos en casos de acoso repetido a y entre menores, con las redes sociales como medio comisivo muy habitual, *vid.* Miró Llinares (2013, pág. 65 y sig.). Antes de la creación de tipos más específicos de acoso, no era extraño en la jurisprudencia, sobre todo de menores, el recurso a los delitos contra la intimidad en supuestos que claramente no satisfacían los requisitos del artículo 197 (a modo de ejemplo, SAP Murcia 7/2010, de 29 de enero).
24. SAP Barcelona 314/2015, de 8 de abril.
25. SAP Pontevedra 320/2017, de 12 de diciembre (entrada a la página de Facebook de su expareja y apertura de mensajes privados que este se intercambia con otra mujer). Se condena (incorrectamente) por el artículo 197.2 y ni siquiera se plantea la concurrencia de intrusismo informático.
26. Pensemos en el caso (bien real) de jóvenes que cuelgan en su Instagram o en su muro de Facebook imágenes en las que aparecen consumiendo droga (por ejemplo, fumando marihuana).



asideros para valorar la posibilidad de que el tipo abarque las conductas que nos ocupan).<sup>27</sup>

### 3.2. Las dificultades interpretativas del intrusismo informático del artículo 197 bis. Su proyección sobre la valoración de la conducta de acceso no consentido al espacio de un usuario en una red social

La introducción en nuestro ordenamiento del delito de *hacking* o intrusismo informático por la LO 5/2010, y su posterior reforma por la LO 1/2015, ha generado una notable controversia doctrinal en torno a la delimitación del bien jurídico protegido por el artículo 197 bis, en la que juega un papel destacado la ubicación sistemática del precepto en la que el legislador ha persistido (pues incluso tras la reforma de 2015 continúa situándolo en el capítulo de los delitos contra la intimidad). El ejemplo de la conducta de acceso no consentido a una red social puede servir como buen botón de muestra de las dificultades interpretativas (inevitables a la luz de la función teleológica desempeñada por el bien jurídico) a que todo ello está dando lugar.

Simplificando un tanto la cuestión dadas las limitaciones de espacio a las que debemos sujetarnos en esta contribución, el núcleo del problema se cifra en hasta qué punto la conducta intrusa, para resultar típica, habría de lesionar o siquiera poner en peligro la intimidad ajena, cuestión sobre la que existen indicadores contradictorios. Por una parte, es cierto que la mencionada ubicación sistemática

del precepto en el seno de los delitos contra la intimidad parecería dar pie a la exigencia, siquiera en clave de generación de un peligro, de una conexión con dicho bien jurídico, y en ese sentido se pronuncia un sector importante de la doctrina, que también suele aludir al carácter excesivamente indeterminado del bien jurídico seguridad informática.<sup>28</sup> De otro lado, sin embargo, parece claro que tal vinculación *excluyente* al bien jurídico intimidad no se corresponde con el sentido de la normativa internacional origen de la tipificación del intrusismo, que indudablemente –baste leer los detallados considerandos de la Directiva 2013/40/UE– apunta a la seguridad informática como bien jurídico protegido en tanto presupuesto imprescindible de la actividad económica y social, los servicios públicos e infraestructuras, la seguridad nacional, etc.;<sup>29</sup> un bien jurídico instrumental (con todo lo que ello pueda tener de discutible, sin duda, en tanto exponente –uno más entre tantísimos otros incorporados a nuestro Código penal en los últimos años<sup>30</sup>– de un claro adelantamiento de las barreras penales de protección), al servicio de múltiples intereses que a mi entender abarcan pero a la vez exceden con mucho la intimidad.<sup>31</sup> La opción por este bien jurídico, de contornos ciertamente poco precisos, obliga de *lege lata*, por descontado, a una interpretación restrictiva del precepto en aras de su compatibilización (ha de reconocerse que compleja) con el principio de ofensividad; de modo provisional, puesto que la cuestión merece un desarrollo mucho más detenido, podrían sugerirse algunas posibilidades en este sentido, que aplicaremos ya sobre el ejemplo del acceso no consentido al espacio de un usuario en una red social.<sup>32</sup>

27. Vid. los hechos de la ya citada SAP Vigo 462/2017, en los que parece que el autor se introduce en la página de Tuenti de su expareja, sin que conste apertura de mensajes privados. En todo caso, la sentencia no se plantea el intrusismo informático; sí condena en cambio por delito contra la integridad moral al haber colgado mensajes procaces haciéndose pasar por la víctima para conseguir hacerla objeto de contactos por terceros.
28. Por todos, Doval Pais y Anarte Borrallo (2016, pág. 517-520); esta parece ser la postura finalmente de Colás Turégano (2016, pág. 218). Vid. igualmente las amplias reflexiones de de la Mata Barranco y Barinas Ubiñas (2014, pág. 59 y sig.) y las de Galán Muñoz (2009, pág. 93-98), que opta por la inviolabilidad informática como bien jurídico claramente individual, desde una perspectiva en todo caso muy crítica con la marcada tendencia del legislador a escudarse en la normativa internacional como coartada de opciones político-criminales, como en este caso, excesivamente expansivas.
29. Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (base de la tipificación de 2010).
30. Muy ilustrativo al respecto el reciente trabajo de Alonso Rimo 2017, con mención expresa en pág. 53 del artículo 197 *ter*, que el autor considera, a diferencia de lo aquí propuesto, tipificación expresa de actos de preparación de delitos contra la intimidad.
31. Por esta configuración del bien jurídico me decantaba en Tomás-Valiente Lanuza (2015, pág. 675). En este sentido también, entre otros, Carrasco Andriano (2010, pág. 249), o Jorge Barreiro y Guérez Tricarico (2017, n.m. 9947).
32. Imprescindible sobre la tipicidad como intrusismo del acceso a redes sociales, Jorge Barreiro y Guérez Tricarico (2017, ns. ms. 9945-9950). Vid. igualmente Picotti (2013, pág. 86-88), a favor de la tipicidad como intrusismo informático (en la legislación italiana) de la entrada no consentida en el espacio de un usuario en la red social.

En primer lugar, podría proponerse una interpretación que exija una especial insidiosidad del medio de acceso al sistema informático, que acentúe el desvalor objetivo de acción y revele una mayor energía criminal en la conducta de vencer las barreras de protección dispuestas por el titular del sistema de información: de acuerdo con esta idea, la entrada en el sistema habría de producirse gracias a una especial destreza o habilidad informática, lo que excluiría del tipo los accesos posibilitados por el hecho de que el sujeto simplemente conozca o disponga de la contraseña (si de este mecanismo de protección se trata) establecida por el usuario, sea porque en algún momento del pasado se le ha permitido tenerla, porque ha observado al usuario tecleándola, etc., supuestos que en puridad no habrían de considerarse *hacking*; precisamente esto es lo que ocurre en la mayoría de los casos (todavía pocos) de entrada no consentida en redes sociales que han llegado a los tribunales, protagonizados por quien había sido pareja del titular de la cuenta (casos en los que, sin embargo y en contra de lo aquí propuesto, se ha tendido a la condena).<sup>33</sup>

Un segundo criterio de reducción teleológica del tipo pasaría por exigir de la conducta la constatación de su peligrosidad para algún bien jurídico identificable (ya sea de titularidad individual -intimidad en el caso que ahora nos interesa- o colectiva -buen funcionamiento de servicios públicos o infraestructuras esenciales, etc.). En lo que aquí importa, no puede perderse de vista, como indican Jorge Barreiro y Guérez Tricarico, la gran diversidad de grados y

matices con que la intimidad personal puede verse afectada por la participación en una red social, pues junto con espacios susceptibles de acoger informaciones más próximas a lo íntimo -la cuenta de usuario de redes como Facebook o Tuenti- existen otros en los que la implicación puede considerarse mínima -chats o foros sobre temas irrelevantes.<sup>34</sup>

En tercera instancia, el elemento típico del vencimiento de medidas de protección (reflejo de ese especial desvalor de acción antes aludido, pero también de la exigencia al titular del sistema de información de la puesta en práctica de sus deberes de autoprotección) se muestra susceptible de interpretaciones más o menos restrictivas. En esta línea podría considerarse atípico, por ejemplo, el acceso a lo protegido con medios fácilmente vencibles; en el ámbito de las redes sociales, esto sucedería cuando el usuario no hubiera hecho uso adecuado de las herramientas de configuración de la privacidad ofrecidas por la red.<sup>35</sup>

Por último, ya en el ámbito concursal, en tanto tipo de peligro para bienes jurídicos identificables más allá del bien instrumental de la seguridad informática, el desvalor del delito de acceso habría de estimarse absorbido por la consumación de otros delitos a los que se encuentre preordenado, lo que, como se ha indicado ya, sucederá -en el caso de entrada en redes sociales- siempre que se abran mensajes intercambiados en privado entre el titular y un tercero, que darán lugar al delito contra la intimidad del artículo 197.1.<sup>36</sup> En este contexto concursal, si el intruso

- 
33. Vid. SAP Álava 74/2013, de 7 de marzo (que confirma la condena en un caso de entrada en Facebook de la expareja, en el que, aunque no se explicita, parece que la contraseña se conocía previamente); SAP Girona 504/2014, de 22 de septiembre (que parte de la tipicidad como intrusismo informático de la entrada en Facebook -parece que también en los casos aludidos en el texto-, si bien finalmente absuelve por no estar probada la falta de autorización); SAP Girona 358/2015, de 22 de junio (que condena por intrusismo la entrada en la página de Facebook de su expareja, cuya contraseña conocía al haber visto a esta última tecleándola). Vid. en cambio SAP Vigo 462/2017, a raíz de lo que parece una entrada no consentida en la página de Tuenti de la expareja, sin que se plantee el intrusismo (sí se condena en cambio por delito contra la integridad moral al haber colgado el autor mensajes procaces haciéndose pasar por la mujer para que fuera objeto de contactos por terceros, como efectivamente ocurrió). Considera que una entrada en la página de Tuenti sí hubiera sido típica de intrusismo de haberse encontrado ya en vigor el delito, SAP Madrid, 402/2012, de 17 de julio.
34. Jorge Barreiro y Guérez Tricarico (2017, ns. ms. 9945 y 9949). Irrelevancia que no puede predicarse por igual de todos los foros o chats (piénsese, por ejemplo, en chats privados sobre preferencias sexuales).
35. En este sentido, entienden Jorge Barreiro y Guérez Tricarico (2017, n.m. 9950), que, de considerarse inicialmente típica la entrada no autorizada en un chat privado (así, la realizada por un inicial usuario luego vetado), la afirmación final de la tipicidad dependería del grado de complejidad del «baneo» o barrera impuesta, pues algunas modalidades resultan muy fácilmente superables por un usuario medianamente avezado.
36. Lo mismo sucederá si al intrusismo sigue la comisión de otros delitos, como (por citar el ejemplo que parece más relevante) daños informáticos del artículo 264 Cp. De hecho, es esta figura (y sobre todo el tipo cualificado de su apartado 2, en sus circunstancias 3.ª y 4.ª, cuando los daños informáticos hayan perjudicado gravemente servicios esenciales, o hayan afectado al sistema informático de una infraestructura crítica, o se hubiera creado una situación de peligro grave para la seguridad del Estado o de la UE) la que parece conectarse de modo más directo con el espíritu de la Directiva.

accede a los datos personales facilitados por el usuario en la configuración de su perfil (dirección de correo electrónico, dirección postal, número de teléfono, profesión, etc.) podría quizás plantearse la entrada en juego del artículo 197.2 (puesto que aquí sí sería más defendible entender que se encuentran archivados en un registro informático); ello dependerá, no obstante, del entendimiento más o menos restrictivo que se defienda de los «datos personales

reservados» objeto material de dicho delito, que a mi entender, como ya he defendido en otro lugar, no deben identificarse sin más con los datos personales objeto de protección administrativa.<sup>37</sup> Al no aplicarse entonces el tipo directamente protector de la intimidad, queda abierta la subsunción de la conducta bajo el intrusismo del 197 bis, que en todo caso convendría sujetar a los parámetros restrictivos arriba mencionados.

## Bibliografía

- ALONSO RIMO, A. (2017). «¿Impunidad general de los actos preparatorios? La expansión de los delitos de preparación». *InDret* 4/2017, pág. 1-79
- CARRASCO ANDRINO, M. (2010). «El delito de acceso ilícito a los sistemas informáticos (arts. 197 y 201)». En: F. J. ÁLVAREZ GARCÍA y J. L. GONZÁLEZ CUSSAC. (dirs.). *Comentarios a la Reforma Penal de 2010*. Valencia: Tirant lo Blanch, pág. 249-256.
- COLÁS TURÉGANO, A. (2016). «El delito de intrusismo informático tras la reforma del Código penal español de 2015». *Revista Boliviana de Derecho*. N.º 21, pág. 210-229.
- DE LA MATA BARRANCO, N.; BARINAS UBIÑAS, D. (2014). «La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?». *Revista de Derecho penal y Criminología*, 3.ª época. N.º 1, pág. 13-92.
- DOVAL PAIS, A.; ANARTE BORALLO, E. (2016). «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio (I). Delitos de descubrimiento y revelación de secretos». En: J. BOIX REIG. *Derecho penal Parte Especial*, vol. I, 2.ª ed. Madrid: lustel, pág. 493-549.
- GALÁN MUÑOZ, A. (2009). «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales». *Revista Penal*. N.º 24, pág. 90-107.
- GONZÁLEZ COLLANTES, T. (2015). «Los delitos contra la intimidad tras la reforma de 2015: luces y sombras». *Revista de Derecho penal y Criminología*, 3.ª Época. N.º 13, pág. 51-84.
- JAREÑO LEAL A. (2008). *Intimidación e imagen: los límites de la protección penal*. Madrid: lustel, 144 pág.
- JORGE BARREIRO, A.; GUÉREZ TRICARICO, P. (2017). «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En: F. MOLINA FERNÁNDEZ (dir.). *Memento penal 2017*. Madrid: Francis Lefevre, ns. ms. 9850-10039.
- MENDO ESTRELLA, A. (2016). «Delito de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos». *Revista Electrónica de Ciencias Penal y Criminología*. N.º 18-16, pág. 1-27.
- MIRÓ LLINARES, F. (2013). «Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio». En: M. J. PIFARRÉ (coord.). «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 16, pág. 61-75.

37. Tomás-Valiente Lanuza (2015, pág. 664-5), donde me acojo a interpretaciones restrictivas del objeto material del artículo 197.2 como la sugerida por Jareño Leal (2008, pág. 61 y sig.).



- MORALES PRATS, F. (2016). «Comentario al art. 197 Cp». En: G. QUINTERO OLIVARES F. MORALES PRATS (2016). *Comentarios al Código penal de 1995. Tomo I, pág. 1434-1473*. 7.ª ed. Cizur Menor: Aranzadi.
- PICOTTI, L. (2013). «Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales». En: M. J. PIFARRÉ (coord.). «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 16, pág. 76-90.
- TOMÁS-VALIENTE LANUZA, C. (2015). «Capítulo I. Del descubrimiento y revelación de secretos». En: M. GÓMEZ TOMILLO. *Comentarios prácticos al Código penal*, Tomo II. Cizur Menor: Aranzadi, pág. 653-698.

### Cita recomendada

TOMÁS-VALIENTE LANUZA, Carmen (2018). «Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 30-41. UOC [Fecha de consulta: dd/mm/aa]  
<http://dx.doi.org/10.7238/idp.v0i27.3147>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre la autora

Carmen Tomás-Valiente Lanuza  
 carmen.tomas-valiente@uib.es

Profesora titular de Derecho Penal  
 Universitat de les Illes Balears

<http://www.uib.es/es/personal/ABjMzNTQwMw/>

Facultat de Dret (edifici Gaspar Melchor de Jovellanos)  
 Universitat de les Illes Balears  
 Cra. de Valldemossa, km 7.5. Palma (Illes Balears)

**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## ARTÍCULO

# El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento

Beatriz López Pesquera  
Agencia provincial de Barcelona  
UOC

Fecha de presentación: mayo de 2018  
Fecha de aceptación: julio de 2018  
Fecha de publicación: septiembre de 2018

**Resumen**

Con ocasión de las ventajas que ofrecen las tecnologías de la sociedad de la información y las redes sociales han proliferado conductas ilícitas centradas, principalmente, en delitos patrimoniales. Las conductas más habituales son aquellas destinadas a la compraventa de productos de segunda mano, las que exponen un modo de vida constituyéndose en *influencers*, o los delitos relativos a la publicidad engañosa, entre otros, aunque el abanico delictual es mucho más amplio. El estudio desvela que, en cualquier caso, no se trata de estafas informáticas propiamente dichas; el número de perjudicados es muy numeroso, existiendo, además, importantes dificultades en su investigación, por no mencionar la concurrencia de problemas concursales en no pocos casos.

**Palabras clave**

redes sociales, estafa, delito informático, delitos patrimoniales

**Tema**

Derecho penal

## Fraud committed via social networks: research and indictment problems

### Abstract

There has been a rise of illegal acts based on the advantages offered by ICT and social networks, mainly based on crimes against property. The most common acts are those relating to the purchase or sale of second-hand products, those exhibiting an influencer lifestyle or crimes relating to misleading advertising, among others. However, the complete range of crimes is much broader. The study reveals that, in any case, these are not ICT scams per se, as the number of parties suffering damages is very high. Its research also poses significant difficulties, as in many cases it does not mention the occurrence of bankruptcy problems.

### Keywords

social networks, fraud, computer crime, crimes against property

### Topic

Criminal Law

## 1. Aproximación a los conceptos

En el presente trabajo trataremos de analizar los principales problemas que la investigación y el enjuiciamiento de los delitos de estafa cometidos a través de las redes sociales plantean. Sin embargo, con carácter previo convendría definir algunos conceptos.

El **delito de estafa** aparece recogido en el artículo 248.1 del Código penal, según el cual «cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno».

El Tribunal Supremo ha enumerado los elementos exigidos en el tipo penal en el artículo 248.1 del Código penal en numerosas ocasiones:<sup>1</sup>

1. Un engaño precedente o concurrente.
2. Dicho engaño ha de ser bastante para la consecución de los fines propuestos, con suficiente entidad para provocar el traspaso patrimonial.

3. Producción de un error esencial en el sujeto pasivo, desconocedor de la situación real.
4. Un acto de disposición patrimonial por parte del sujeto pasivo, con el consiguiente perjuicio para el mismo.
5. Nexo causal entre el engaño del autor y el perjuicio a la víctima.
6. Ánimo de lucro.

El elemento característico del delito de estafa, como es bien sabido, es el «engaño bastante». La jurisprudencia del Tribunal Supremo ha venido configurando el engaño típico en no pocas sentencias<sup>2</sup> como «aquél que genera un riesgo jurídicamente desaprobado para el bien jurídico tutelado y concretamente el idóneo o adecuado para provocar el error determinante de la injusta disminución del patrimonio ajeno».

En torno al engaño bastante se han suscitado muchas cuestiones que exceden del objeto de este trabajo; sin embargo, me gustaría poder traer a colación alguna de ellas por la relevancia que pueda tener en los supuestos que se analizarán.

1. Vid. STS 810/2016, de 28 de octubre, con cita, entre otras a la STS 880/2005, de 4 de julio.  
2. Vid. SSTS 564/2007, 162/2012, de 23 de diciembre.

Se ha planteado la autotutela como causa de exclusión de la tipicidad en estos delitos, si bien el Tribunal Supremo ha establecido<sup>3</sup> que una cosa es la exclusión del delito de estafa en supuestos de «engaño burdo» o de «absoluta falta de perspicacia, estúpida credulidad o extraordinaria indolencia», y otra que se pretenda desplazar sobre la víctima de estos delitos la responsabilidad del engaño, exigiendo un modelo de autoprotección o autotutela que no está definido en el tipo penal ni se reclama en otras infracciones patrimoniales. No resulta procedente, por ello, renunciar a la intervención penal a favor de la autotutela de la víctima, desconociendo que constituye un principio básico del ordenamiento jurídico el de que los ciudadanos han hecho dejación de la respuesta punitiva en manos del Poder Judicial precisamente para descargarse de sus necesidades defensivas frente a las agresiones legalmente tipificadas como delictivas.

La configuración del concepto «engaño bastante para producir error en otro» implica la necesaria relación entre un sujeto activo y un sujeto pasivo. Antes del Código penal de 1995, dicha configuración planteaba problemas tanto para la doctrina como para la jurisprudencia al tratar de calificar jurídicamente determinados hechos, fundamentalmente las transferencias no consentidas de dinero ajeno, puesto que se partía de la premisa de que no se podía engañar a una máquina.

Como decíamos, el Código penal de 1995, ya en su redacción original, vino a resolver la cuestión en el apartado 2.º del artículo 248 CP tipificando las denominadas estafas impropias de la siguiente manera: «También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero»; por su parte, el apartado 3.º del artículo 248 CP establecía que se aplicaría la misma pena «a los que fabricaren, introdujeran, poseyer-

ren o facilitaren programas de ordenador especialmente destinados a la comisión de las estafas previstas en este artículo» (conductas, estas últimas, en las que no se habría producido perjuicio patrimonial alguno, todavía).

El vigente artículo 248.2 del Código penal engloba los originales apartados 2.º y 3.º y añade una conducta más, sancionada con idéntica pena para «los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero».

Por lo que respecta al concepto de **delitos informáticos**, el Convenio sobre Cibercriminalidad (Budapest, 23 noviembre de 2001), en el seno del Consejo de Europa,<sup>4</sup> en su preámbulo indica la necesidad de establecer mecanismos de prevención, incriminación de las conductas en él descritas y atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales.<sup>5</sup>

Podemos conceptualizar los delitos informáticos<sup>6</sup> como «aquellas conductas típicas, antijurídicas, culpables y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores, computadoras o cualquier otro mecanismo electrónico o informático, bien como medio, bien como fin, o mediante el uso indebido de los mismos».

El Convenio de Budapest nos ofrece un concepto de **estafas informáticas** en su artículo 8, indicando que «los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

- a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

3. Vid. SSTS 162/2012, de 15 de marzo; 243/2012, de 30 de marzo; y 344/2013, de 30 de abril.

4. Instrumento de ratificación publicado en el BOE de 17 de septiembre de 2010.

5. En el preámbulo del Convenio de Budapest se indica la necesidad del mismo: «Para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable».

6. Así los conceptúa Rey Huidobro (2013).

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona».

Dentro del concepto «estafas informáticas» propiamente dichas podemos incluir el *phising*, el *smishing* y el *pharming*, cuyo estudio excede del objeto de este trabajo.<sup>7</sup>

La RAE define **red social** como la plataforma digital de comunicación global que pone en contacto a un gran número de usuarios. Si acudimos al Observatorio Tecnológico del Ministerio de Educación, Cultura y Deporte, encontramos una definición más extensa: se trata de «estructuras sociales compuestas por un grupo de personas que comparten un interés común, relación o actividad a través de internet, donde tienen lugar los encuentros sociales y se muestran las preferencias de consumo de información mediante la comunicación, en tiempo real, aunque también puede darse la comunicación diferida en el tiempo, como en el caso de los foros».<sup>8</sup>

## 2. Las estafas y las redes sociales. Problemas prácticos en su investigación

Resulta una obviedad señalar que, en los últimos años, hemos asistido a la proliferación de las redes sociales en

general y a la de aquellas destinadas a la compraventa de productos de segunda mano, en particular. Es en el ámbito de estas últimas donde fijaremos nuestra atención para analizar los problemas que se suscitan ante la comisión de delitos de estafa.

En la estafa «tipo» de la que se parte, la básica, una persona, el vendedor, oferta un producto determinado en una red social, entra en contacto con el comprador, quien deberá efectuar el ingreso de la cantidad concertada con carácter previo a la recepción del producto, si bien dicho producto nunca llegará a su destinatario, quien tras varios intentos, todos ellos infructuosos, por resolver el problema, finalmente, en el mejor de los casos, optará por interponer la denuncia correspondiente. En otras modalidades, el comprador efectúa el ingreso acordado, o bien, lo hace a cargo de la cuenta de un tercero desconocedor de la operación, o lo hace a cargo de una cuenta bancaria de su titularidad (real o ficticia, con lo que podríamos encontrarnos ante otros ilícitos penales); efectuado el ingreso y remitido el comprobante al vendedor, una vez obtiene el producto en cuestión, anula el cargo o este es anulado por el titular de la cuenta bancaria ajeno a la defraudación cuando se percata del cargo.

La primera cuestión que podemos plantearnos es si estamos ante auténticas estafas informáticas; la respuesta, en términos generales, debe ser negativa, como ya se apuntaba en la Instrucción FGE 2/2011.<sup>9</sup> Se trata de estafas comunes, sin perjuicio de que se haya utilizado la tecnología para su comisión (básicamente, para que el sujeto activo

7. Véase Velasco Núñez (2008).

El *phising*, generalmente, se realiza enviando mensajes de correo electrónico reportados desde diversos sitios de la red (pero también a través de virus o enlaces de páginas web), principalmente a usuarios de la banca informática en cuyos textos, haciéndose pasar por los servicios de seguridad del banco, apremian y urgen a los usuarios –a veces bajo amenazas de anular la cuenta– a conectarse a una página web perfectamente imitada, pero falsa, y en ella a ceder los códigos de acceso y contraseñas secretas de seguridad, que una vez conocidas por los delincuentes, les permiten usarlas y quedarse con el dinero de sus víctimas. [...] En el *smishing* (*phising* por SMS) se suelen enviar los mensajes a través del teléfono móvil y lo que se pide en sus textos engañosos son el número de tarjeta y la fecha de caducidad, con esa información se confeccionan tarjetas de crédito falsas (*skimming*) para adquirir productos en el mercado, cargados contra la cuenta asociada del engañado. [...] El *pharming* consiste en una modificación técnica de las direcciones DNS (*domain name server*) del servidor informático o del archivo *host* del PC, hecha por el *pharmer*, tras la que, quien teclea en la barra del buscador las señas (generalmente de bancos en línea) no accede a la página web solicitada, sino a otra perfectamente imitada a la que el servidor le redirecciona y en la que se ponen sin querer y sin saber los datos y claves secretas del usuario bancario, por creer estar usando sus servicios al creer estar en la web del banco, claves que luego son usadas por el delincuente para realizar a su favor transferencias no consentidas por el titular, a quien le indican que en ese momento no pueden atender por razones técnicas.

8. Véase Ponce Idatzia (2012).

9. La Instrucción 2/2011, de la Fiscalía General del Estado, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, tras exponer la necesidad de la especialización en esta materia, configura el marco competencial de la misma y señala que «efectivamente, junto a tipos penales a través de los cuales el legislador ha protegido específicamente la seguridad de

y el pasivo entren en contacto), pero sin que haya existido una manipulación informática o un artificio semejante, como exige el apartado 2.º del artículo 248 CP.

El encontrarnos ante estafas comunes no implica que no se susciten problemas prácticos. Hace años, un ladrón atracaba un banco y robaba un millón de euros; ahora, ese mismo ladrón, sin necesidad de salir de su casa, puede robar un euro a un millón de personas. Esta nueva realidad conlleva una problemática propia en la investigación de tales hechos. En primer lugar, no se puede ignorar el riesgo de impunidad de muchas de estas conductas precisamente por la escasa cuantía de alguno de estos fraudes que determina que las víctimas opten por no denunciar el delito, que ponderen el perjuicio económico sufrido con las molestias/inconvenientes que les puede suponer interponer una denuncia e iniciar, así, un procedimiento penal.

A ello debemos añadir que el número de potenciales víctimas de estas estafas puede ser elevado, puesto que serán tantas como pudieran tener acceso a la información difundida y la dispersión geográfica de las mismas, lo que puede acentuar el riesgo de impunidad del que hablábamos anteriormente.

Superado el momento de interponer la denuncia por la víctima, aparecen nuevas cuestiones.

El Acuerdo del Pleno no jurisdiccional del Tribunal Supremo del 3 de febrero de 2005 resolvió la cuestión de la competencia para la instrucción de los delitos de estafa al consagrar la regla de la ubicuidad, según la cual «el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo; en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa».

Uno de los principales problemas a la hora de investigar una estafa de este tipo radica en la dificultad para identificar y localizar al presunto autor de la misma. Partiendo de

la estafa «tipo» que hemos descrito en párrafos anteriores, si el sujeto facilitó un número de cuenta donde efectuar el ingreso de su titularidad, la identificación resultará sencilla, puesto que la entidad bancaria en cuestión indicará la titularidad de esta y la dificultad radicarán en la localización de esa persona para que preste declaración en sede judicial en calidad de investigado. Si el número de cuenta facilitado pertenece a un tercero, se deberá dilucidar si ese tercero corresponde a una persona real o ficticia y, en el primer caso, si actuó en connivencia con el autor, lo que nos conduciría a cuestiones relativas a la autoría y participación en el delito.

La identificación del autor, para el caso de que los datos bancarios facilitados fueran falsos o pertenecientes a un tercero ajeno al fraude, debería realizarse a través de la investigación de la IP desde la que se emitió el anuncio en cuestión. En este punto, debemos indicar que también se suscitan problemas en la práctica. Bien es cierto que contamos con la nueva regulación, entre otras, de lo establecido en el artículo 588.ter de la Ley de Enjuiciamiento Criminal, específicamente el artículo 588.ter.k LEcrim y en el artículo 588.octies LEcrim, pero hemos de tener en cuenta las limitaciones temporales establecidas en este último («los datos se conservarán durante un período máximo de noventa días, prorrogables una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días»). Asimismo, debemos tener presente lo dispuesto en el artículo 5 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, según el cual «la obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores»; norma que debe ser interpretada

---

los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan por tanto, a los efectos de su investigación y/o enjuiciamiento singularidades y dificultades similares a las de los primeramente indicados. No obstante, esta circunstancia no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa».



a la luz de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 21 de diciembre de 2016.<sup>10</sup>

Como resulta sencillo deducir, en este tipo de estafa el autor de la misma ofrece el mismo producto a una pluralidad de personas, como decíamos, por lo que se cometerán tantos delitos de estafa como víctimas hayan contactado con el estafador. Quizás la respuesta penal que deberían tener tales supuestos sería la de su investigación y enjuiciamiento en un único procedimiento que permitiera comprender la dimensión real del ilícito, respuesta que no siempre se produce en la práctica donde el procedimiento se limita a un único delito, en la mayoría de los casos.

La dispersión geográfica de las víctimas es uno de los elementos que explican la dificultad para investigar este tipo de estafas de manera conjunta en un único procedimiento. La existencia de una pluralidad de víctimas en diferentes puntos de la geografía (sin contar con la posibilidad de que alguna de ellas pueda residir en el extranjero, circunstancia que añadiría nuevas dificultades en la investigación) implicaría la necesidad de realizar actuaciones judiciales en muchos casos mediante exhortos, lo que dilataría el procedimiento inevitablemente; si bien, esta dificultad podría verse mitigada con la declaración de complejidad de la causa en los términos del artículo 324 LEcrim.

En caso de investigarse y enjuiciarse en un único procedimiento una pluralidad de estafas, no existe óbice para considerar que se trataría de un delito continuado en los términos del artículo 74 CP: «El que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de acciones u omisiones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza».<sup>11</sup>

Cuestión distinta será ventilar la relación existente entre lo dispuesto en el artículo 74 CP y el subtipo agravado del artículo 250.1.5 CP (que «el valor de la defraudación supere los 50.000 euros o afecten a un elevado número de personas»).

El Acuerdo del Pleno no jurisdiccional del Tribunal Supremo de fecha 30 de octubre de 2007 estableció que «el delito continuado siempre se sanciona con la mitad superior de la pena. Cuando se trata de delitos patrimoniales la pena básica no se determina en atención a la infracción más grave, sino al perjuicio total causado. La regla primera, artículo 74.1 CP queda sin efecto cuando su aplicación fuera contraria a la prohibición de doble valoración».

Como ha venido entendiendo la jurisprudencia,<sup>12</sup> el delito continuado recoge el mayor contenido del injusto derivado de la constatación de una comisión sucesiva y reiterada de unas conductas agresivas a un mismo bien jurídico, bajo un dolo único y aprovechamiento de idénticas circunstancias. Es obvio que esa conducta, caracterizada por la concurrencia de los presupuestos del delito continuado, merece un mayor reproche penal. Desarrollando el citado Acuerdo del Pleno no jurisdiccional del Tribunal Supremo de fecha 30 de octubre de 2007, la jurisprudencia ha entendido, como se recogía ya en la STS 950/2007, de 13 de noviembre, que «cuando se trata de infracciones patrimoniales, la pena se impondrá teniendo en cuenta el perjuicio total causado conforme dispone el artículo 74.2 CP. De manera que si la suma de ese perjuicio es superior a 36.000 euros (actualmente 50.000 euros), la pena procedente es la prevista en el artículo 250.1.6º (actual artículo 250.1.5º CP) y si es inferior a esa cifra la del artículo 249 [...]. Cuando esa cifra (la relevante para incrementar la pena básica) se alcanza por la suma de las diferentes infracciones, acudir a la agravación del apartado 1 del artículo 74 vulneraría la prohibición de doble valoración de una misma circunstancia o de un mismo elemento, pues de un lado se ha tenido en cuenta para acudir al artículo 250.1.6ª CP (actual artículo 250.1.5º CP), con la consiguiente elevación de la pena [...] y de otro se valoraría para acudir al artículo 74.1 CP, agravándola nuevamente. Ello conduciría a determinar la pena conforme al perjuicio total causado pero sin que fuera preciso imponerla en su mitad superior, de forma que el Tribunal podría recorrer la pena en toda su extensión».

10. La STJUE (Gran Sala) de 21 de diciembre de 2016 ha declarado contrarios a la Carta Europea de Derechos Humanos, en concreto a sus artículos 7, 8, 11 y 52.1, regímenes de conservación preventiva de datos relativos a las comunicaciones basados, como nuestra Ley 25/2007, en la implementación de la Directiva 2006/22/CE, declarada inválida por la STJUE (Gran Sala) de 8 de abril de 2014.

11. Cuestión que ya fue tratada en la Consulta FGE 3/1999, de 17 de septiembre, sobre la pena que procede imponer a las infracciones penales continuadas de carácter patrimonial.

12. Vid. STS 950/2007, de 13 de noviembre; STS 226/2007, de 16 de marzo, entre otras.



En relación con el delito masa, como modalidad agravada del delito continuado, con características específicas que le dotan de una autonomía y sustantividad propias,<sup>13</sup> cabe decir que, *a priori*, no hay obstáculo alguno para apreciarlo si concurren los elementos para ello; esto es, el dolo preconcebido (a diferencia del delito continuado, en el que se admite el dolo ocasional exteriorizador del que aprovecha idéntica ocasión) y los elementos propios del delito con sujeto pasivo masa, a saber, la notoria gravedad (gravedad económica) y la generalidad de personas (grupo numeroso de personas, incluso indeterminado, destinatarios de la actividad ilícita del autor). En este sentido, la STS 719/2010, de 20 de julio, afirmaba que «el llamado delito masa existe cuando un solo acto inicial del sujeto activo determina que acudan a él una pluralidad indeterminada de personas, como puede ocurrir en casos de publicidad engañosa».

Atendiendo a las características del tipo de estafas que analizamos, parece difícil encontrar en la práctica un supuesto de delito masa, pero ello no significa que sea totalmente imposible.

Otra de las cuestiones que deberíamos analizar es la posibilidad de que a través de las redes sociales se cometa una estafa piramidal;<sup>14</sup> partiendo de la utilización de las redes sociales como plataforma a través de la cual se pueda acceder al mayor número de potenciales víctimas.

### 3. Las redes sociales y otras posibles conductas típicas de contenido patrimonial

Cuando las conductas analizadas se incardinan en el seno de una organización o de un grupo criminal, más allá de los supuestos de mera coautoría, no habría inconveniente en calificar tales conductas conforme a lo dispuesto en el artículo 570.bis CP<sup>15</sup> (organización criminal) o en el artículo 570.ter CP<sup>16</sup> en su caso (grupo criminal).

Hasta el momento, nos hemos centrado en las estafas cometidas a través de redes sociales dedicadas a la compraventa de productos, generalmente, de segunda mano, pero ¿y a través de otras redes sociales como Instagram?

En este caso la estafa que denominamos «tipo» estaría dirigida, en su gran mayoría, a aquellas empresas que pretenderían publicitar sus productos por medio de los/ las *influencers*.

No podemos dejar a un lado el hecho de que, evidentemente, no todo lo que se publica en Instagram corresponde con la realidad, es decir, una persona puede crearse un perfil y mostrar a través de sus fotografías y sus vídeos una vida que no es real, que no se corresponde con la suya, pero

13. Vid. STS de 10 de junio de 2014.

14. Vid. STS 324/2012 de 10 de mayo: «El autor de una estafa lesiona un deber de respeto de la organización del sujeto pasivo cuando le presenta una situación de hecho que induce a dicho sujeto a obtener falsas conclusiones. En los casos en que el actor propone a la víctima invertir en su negocio, le corresponde al actor ofrecer información veraz sobre los elementos básicos del negocio de que se trate, pues por la posición que ocupa en la relación, es el actor el único que dispone de esta información, que no es normativamente accesible a la víctima.

Por ello considera la mejor doctrina que debe apreciarse estafa cuando el actor propone a la víctima un negocio inexistente, revistiendo esta propuesta de una puesta en escena que la dota de verosimilitud, y obteniendo así que la víctima le entregue el dinero solicitado, efectuando un desplazamiento patrimonial destinado supuestamente a invertir en el negocio del actor, y recibir el beneficio correspondiente, cuando en realidad la intención del actor es apropiarse directamente del dinero recibido, sin invertirlo en negocio alguno, con notorio perjuicio para la víctima.

Esto es lo que ha sucedido en el caso actual, en el que el recurrente ofrecía a los perjudicados invertir en su negocio elevadas sumas de dinero, a cambio de un interés importante, aparentando solvencia mediante la constitución de una entidad mercantil de inversiones, realizando su oferta con la garantía de un pagaré que supuestamente garantizaba la devolución íntegra del dinero y abonando durante un corto tiempo los intereses prometidos, lo que servía de anzuelo para captar nuevos clientes, con cuyo capital se abonaban los intereses. Este modelo piramidal de estafa conduce necesariamente a la frustración del negocio prometido, pues en la medida que se incrementa el capital recibido, aumentan exponencialmente las necesidades de nuevos ingresos para abonar los intereses, hasta que el actor cesa en el pago de los intereses y se apropia definitivamente de los capitales fraudulentamente recibidos».

15. El artículo 570.bis CP define la organización criminal como «la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se reparten diversas tareas o funciones con el fin de cometer delitos».

16. El artículo 570.ter CP define el grupo criminal como «la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo 570.bis CP, tengan por finalidad o por objeto la perpetración concertada de delitos».

que precisamente esa vida publicitada, los miles de seguidores que pueden acceder a ese perfil y seguirlo, pueda interesar a determinadas empresas que quieran vincular sus productos, y por tanto publicitarlos, con ese estilo de vida, todo ello a cambio de la correspondiente contraprestación económica. El hecho de que la «vida exhibida» no sea real no constituye, *a priori*, un elemento determinante para concluir que podríamos estar ante una estafa. El anunciante lo que pretende es que sus productos lleguen al mayor número de consumidores potenciales y, en este sentido, su objetivo se cumple siempre y cuando los seguidores de la cuenta en cuestión correspondan a personas reales, ajenas a la realidad de la vida del *influencer*. La respuesta cambia si ese número elevado de seguidores que atrae al anunciante son falsos, comprados, no son personas reales, sino simples perfiles inactivos. En este supuesto, sí podríamos sostener que estaríamos ante una estafa. El/la *influencer* hizo creer al anunciante que efectivamente lo era, que tenía miles de seguidores y mediante ese engaño se generó error en aquel que determinó el desplazamiento patrimonial en su perjuicio. El mismo esquema y la misma respuesta obtendrá si lo analizado son las cuentas de YouTube; dependerá si las visitas recibidas son ciertas o no.

A través de las redes sociales podrán cometerse otros delitos de contenido patrimonial, como los delitos contra la propiedad intelectual e industrial (arts. 270 a 277 CP)<sup>17</sup> o los delitos relativos a la publicidad engañosa (art. 282 CP),<sup>18</sup> que encontrarían en ellas un medio en el que desarrollar su actividad de forma extraordinariamente eficaz, si bien su análisis excede con creces el objeto de este trabajo.

No podía finalizar el presente trabajo sin referirme a una conducta que, sin ser propiamente un delito de contenido patrimonial, prolifera en las redes sociales y plantea interesantes problemas concursales (que por razones obvias no entraré a estudiar en este trabajo); me refiero a la comercialización y venta de medicamentos (falsificados

en su mayoría, lo que nos remitiría a los delitos contra la propiedad industrial, así como al delito de publicidad engañosa) a través de las redes sociales (mención aparte merecerían los supuestos de ofertas a través de las redes sociales de drogas tóxicas, estupefacientes o sustancias psicotrópicas, sustancias dopantes). Las redes sociales constituyen la plataforma que permite que el sujeto activo acceda al mayor número de personas posibles. El artículo 361 CP tipifica la conducta del que «fabrique, importe, exporte, suministre, intermedie, comercialice, ofrezca o ponga en el mercado, o almacene con estas finalidades, medicamentos, incluidos los de uso humano y veterinario, así como los medicamentos en investigación, que carezcan de la necesaria autorización exigida por la ley, o productos sanitarios que no dispongan de los documentos de conformidad exigidos por las disposiciones de carácter general, o que estuvieran deteriorados, caducados o incumplieran las exigencias técnicas relativas a su composición, estabilidad y eficacia, y con ello se genere un riesgo para la vida o la salud de las personas».

El artículo 13.d del Convenio del Consejo de Europa sobre la falsificación de productos médicos y delitos similares que supongan una amenaza para la salud pública, hecho en Moscú el 28 de octubre de 2011 (Medicrime),<sup>19</sup> define como una circunstancia agravante de los delitos relativos a la falsificación de medicamentos, que «los delitos de suministro y oferta de suministro se hubiesen cometido recurriendo a medios de difusión a gran escala, tales como los sistemas informáticos, y en particular internet».

## 4. Conclusiones

Comenzamos el presente trabajo fijando conceptos y centrando nuestra atención en las estafas cometidas a través de las redes sociales; en los términos analizados, concluimos que no son estafas informáticas, sino comunes.

- 
17. El artículo 270.2 CP castiga «a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios».
  18. El artículo 282 CP sanciona a «los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos».
  19. Ratificado por España y publicado el Instrumento de ratificación en el BOE de 30 de noviembre de 2015.

El tipo de estafa analizado conlleva problemas prácticos en su investigación, desde la dispersión geográfica de las víctimas, la posible impunidad de determinadas conductas ante la escasa cuantía del fraude, hasta la dificultad para identificar y localizar al autor de tales hechos; cabría la calificación como delito continuado y en teoría como delito masa, aunque resultará difícil encontrarlo en la práctica por sus propias características.

Asimismo, las estafas estudiadas no serían los únicos delitos de contenido patrimonial que podrían ser cometidos a través de las redes sociales, como se han apuntado, resultando interesantes problemas concursales en algunos supuestos, que exceden del presente trabajo.

Como hemos visto, las redes sociales, en los supuestos estudiados, no constituyen elementos definitorios de los delitos analizados, permiten facilitar su comisión, constituyen la plataforma para la toma de contacto entre el sujeto activo y el sujeto pasivo, dificultan, en ocasiones, su investigación, pero ello tampoco debe llevarnos a la demonización de las mismas. Son nuevas herramientas de las que disponemos los humanos y, de la misma forma que debemos aprender a utilizarlas, el ordenamiento jurídico deberá ir dando respuesta a los problemas que vayan planteándose en la práctica.

## Bibliografía

- REY HUIDOBRO, L. F. (2013). «La estafa informática: relevancia penal del *phising* y el *pharming*», *La Ley Penal*, n. 101.
- VELASCO NÚÑEZ, E. (2008). «Estafa informática y banda organizada. *Phising*, *pharming*, *smishing* y "muleros"». *La Ley Penal*, n.º 49.
- PONCE IDATZIA, I. (2012) «Monográfico Redes Sociales». Observatorio Tecnológico. Ministerio de Educación, Cultura y Deporte.

## Cita recomendada

LÓPEZ PESQUERA, Beatriz (2018). «El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 42-51. UOC [Fecha de consulta: dd/mm/aa]  
 <<http://dx.doi.org/10.7238/idp.v0i27.3150>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

---

### Sobre la autora

Beatriz López Pesquera

[blopezpesq@uoc.edu](mailto:blopezpesq@uoc.edu)

Fiscal de la Audiencia Provincial de Barcelona

Profesora colaboradora de la UOC

UOC

Av. Carl Friedrich Gauss, 5

08860 Castelldefels

**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

## ARTÍCULO

# Juicios paralelos en las redes sociales y proceso penal

Vicente C. Guzmán Fluja  
 Universidad Pablo de Olavide

Fecha de presentación: mayo de 2018  
 Fecha de aceptación: julio de 2018  
 Fecha de publicación: septiembre de 2018

## Resumen

Las redes sociales contribuyen a magnificar los juicios paralelos y multiplican las eventuales lesiones de los derechos fundamentales. Ahora bien, es importante determinar si la alimentación que sufren los juicios paralelos a través de las redes añaden algo nuevo a la posible influencia en el transcurso del juicio, siendo un dato a tener en cuenta que cuando se trata de jueces profesionales su permeabilidad se presenta más blindada que frente a los jueces legos. El trabajo revela cuáles son los problemas reales de los juicios paralelos, contextualizándolos debidamente, proponiendo cómo debiera ser abordada su posible regulación.

## Palabras clave

libertad de expresión, redes sociales, prensa, juicios paralelos, intimidad, imagen

## Tema

Derecho procesal penal

## *Parallel trials in social networks and criminal proceedings*

## Abstract

*Social networks help to magnify parallel trials and multiply the eventual breaches of fundamental rights. However, it is important to determine whether or not the parallel trials are potentially influenced by comments on social networks. One point worth considering is that professional judges are harder to influence than lay judges. The study reveals the real problems of parallel trials, duly contextualising them and proposing how their possible regulation should be appropriately dealt with.*

## Keywords

*freedom of expression, social networks, press, parallel trials, privacy, image*

## Topic

*Criminal Procedural Law*

## 1. Juicios paralelos: un problema recurrente y complejo

La aparición y uso generalizado de las redes sociales no es sino un factor más que abunda en la relación conflictiva entre justicia y medios de comunicación y su insano producto: los juicios paralelos. Como es sabido, el uso de las redes sociales se ha convertido en elemento cotidiano en la vida diaria de millones de personas. A través de ellas se producen interacciones instantáneas y continuadas entre un gran número de personas sobre cualesquiera temas que puedan reputarse de interés para ellas. Y son instrumento de información, opinión, conversación, debate, crítica, expresión artística, publicidad, comercio y otras manifestaciones de la creatividad humana, aunque las características propias de cada red social determinan los límites de estas actividades.<sup>1</sup>

En este trabajo se analiza exclusivamente el impacto que las redes sociales causan en relación con procesos penales en curso que resultan objeto de atención por parte de los usuarios de dichas redes.<sup>2</sup> Dicho de otra forma, las redes sociales contribuyen a la generación y expansión de juicios paralelos y, por lo tanto, a la formación de corrientes de opinión pública que, desde la imagen transmitida acerca de lo que acontece en la tramitación del concreto proceso penal, pueden influir, directa o indirectamente, tanto en el desarrollo de dicho proceso como en las decisiones que haya que tomar a lo largo del mismo, como en la percepción social, individual o colectiva, de las personas relacionadas con el caso penal. De esta manera, se generan estados de opinión pública sobre si los policías, fiscales,

jueces, incluso abogados, están haciendo correctamente su trabajo, así como expectativas concretas sobre en qué sentido deben ir tomando decisiones hasta esclarecer definitivamente el hecho delictivo; se pone bajo la lupa el carácter, comportamiento, actividades, ética, moral, del investigado, por supuesto, pero también de la víctima y de los testigos; se comenta cada hallazgo de la investigación, cada declaración personal, cada detalle de la investigación o del juicio que trasciende, y se proyecta cómo influirá cada uno de ellos en la decisión final del caso.

Por lo tanto, se trata de abordar el papel que juegan las redes sociales en la construcción de los juicios paralelos de índole penal desde la necesaria e imprescindible convivencia entre derechos fundamentales reconocidos por la Constitución española: el derecho a la libertad de información del artículo 20.1.d) (muchas veces acompañado de la libertad de expresión u opinión) y los derechos básicos de la personalidad, artículo 18.1, que representan el honor, la intimidad y la propia imagen de las personas relacionadas con un caso penal y sobre las que recae esa información, a los que se suma la presunción de inocencia.

En mi opinión, una relación sana entre justicia y medios de comunicación debe cumplir con el deber de informar de forma precisa, objetiva y veraz sobre procesos judiciales penales en curso y, a la vez, impedir especialmente la existencia de juicios paralelos. Pero debemos ser muy conscientes de que la situación actual dista mucho de ser una relación sana. Y lo cierto, hoy en día, es que todo juicio paralelo es susceptible de convertirse en un producto tóxico capaz de envenenar, más si la información va acom-

1. Por citar algunos datos relevantes referidos a 2017, la red social más usada en el mundo fue Facebook, con 2.000 millones de usuarios, mientras que Twitter, que ocupa el décimo lugar entre las redes sociales más usadas, registraba 350 millones de usuarios. Los puestos dos a nueve los ocupan WhatsApp, YouTube, Wechat, QQ, Instagram, Qzone, Tumblr, LinkedIn. Entre las 30 primeras más usadas aparecen algunas más conocidas, tales como Snapchat, Skipe, Viber, Badoo, Flickr o Spotify, y otras algo menos conocidas como Reddit, Line, Pinterest o Taringa. Cada una de ellas tiene sus peculiaridades de configuración y de posibilidades de comunicación para sus usuarios, por ejemplo, y sin ningún ánimo de exhaustividad: Instagram es una red en la que las imágenes tienen una vital importancia; Twitter restringe la comunicación a 280 (originariamente 140) caracteres por tuit, y permite integrar contenido multimedia; Facebook, entre otras características, es lugar idóneo para que las empresas y corporaciones acerquen sus marcas a los usuarios, fidelizando clientes. Un didáctico y breve ensayo sobre las diferencias entre estas tres redes sociales se encuentra Goetz (2016). Recientemente, en febrero de 2018, se ha revelado la existencia de importantes problemas de uso de datos que constan en las redes sociales para fines diferentes de los que significan el uso de esas redes. Seguramente no es sino la punta del iceberg.
2. Redes sociales y proceso penal se relacionan de otras formas. Por ejemplo, un buen panorama de los delitos cometidos a través de internet, incluidos los cometidos a través de redes sociales en Miró Llinares (2012); téngase en cuenta, en este sentido, la reforma de 2015 del Código penal. Por supuesto, las redes sociales son también fuente y medio de investigación y, después, de prueba en relación con concretos hechos delictivos, véase por ejemplo Barrera (2017). Tampoco se analiza aquí otra interesante perspectiva: internet y las redes sociales como instrumentos de la prevención de comisión de delitos por medio de las investigaciones proactivas y la policía predictiva.

pañada de la opinión, la que debería ser la normal relación democrática libertad de información y justicia.

De sobras es sabido que el proceso penal tiene una fase pública, el juicio oral, y otra secreta, la de investigación-instrucción. Así, desde el momento en que el juicio oral penal es público, la información que se realice sobre el mismo, información, que puede incorporar opinión (terreno más complejo y resbaladizo), puede y debe versar sobre cualquier aspecto, dato, elemento, prueba, declaración, etc., que se haga en el juicio oral.<sup>3</sup> De hecho, es posible, y cada vez resulta más común, la retransmisión en directo de juicios orales penales de forma que, no ya los medios de comunicación, sino el público en general tiene acceso directo a cuanto sucede en la sala de vistas y pueden comentarlo en las redes sociales. Esto no justifica que puedan surgir juicios paralelos mediáticos que proyecten a los estados de opinión pública una imagen distorsionada de lo que está sucediendo en el juicio penal.

Lo que puede y debe hacerse es establecer las reglas que impidan que el juicio paralelo mediático, así como los estados de opinión pública que producen, llegue a influir en el juicio penal, así como garantizar que la libertad de información se ejerce conforme a las reglas éticas de respeto a lo que sucede en el juicio oral, sin tergiversarlo, sin distorsionarlo, sin adelantar conclusiones a partir de los datos que van apareciendo. Se trata no de generar un juicio propio mediático, sino de transmitir de la manera más fehaciente posible qué está sucediendo en la vista del juicio oral.

Desde luego, durante la fase de investigación-instrucción de un concreto caso penal, la fase anterior al juicio oral, no es tolerable que puedan generarse juicios paralelos, aunque es legítimo que se quiera informar sobre la comisión de hechos delictivos y sobre los avances de la investigación criminal (véase STC 14/2003, de 28 de enero). Este derecho de informar (vertiente activa de la libertad de información), que va acompañado del derecho a ser informado (vertiente pasiva), debe ser respetuoso con las reglas procesales penales que rigen la instrucción del proceso penal, sobre todo con la que establece que dicha instrucción es legalmente secreta (actuaciones reservadas y carácter no público, artículo 301 LECrim) para toda persona que no sea parte en el proceso y que además puede ser secreta, si así lo decide el juez y en los términos autorizados por la ley, para las partes personadas exceptuado el Ministerio Fiscal, artículo 302 LECrim.<sup>4</sup> Esto significa que, por ministerio de la ley, la investigación del caso, su instrucción judicial, no son en ningún caso públicas y que el rango operativo del derecho de información es mucho menor que en el caso del juicio oral. Sabido es que hay casos, sobre todo los que levantan grandes expectativas mediáticas, en los que los actos de investigación, las declaraciones de los testigos e investigados, y mucha otra información que figura en la instrucción judicial se hacen de dominio público, y por tanto objeto de información y opinión tanto en los medios de comunicación como en las redes sociales, por efecto de las filtraciones; gravísimo problema que debería abordarse con urgencia de una vez.<sup>5</sup>

3. El artículo 120 CE consagra el principio de publicidad de las actuaciones procesales con las excepciones que se establezcan en la ley. Una buena exposición sobre el tema, así como sobre el secreto sumarial (antes de la reforma de 2015) en Montalvo Albiol (2012, pág. 105-110).
4. El secreto de la instrucción como regla general hacia el público en general, incluidos los medios de comunicación, es una garantía de la persona investigada. En efecto, cuando una persona resulta vinculada con una investigación penal como partícipe hay mucho camino que recorrer hasta que esa vinculación vaya resultando confirmada, de menor a mayor grado hasta que se decide acusar a esta persona y abrir juicio oral contra ella, pudiendo resultar que las investigaciones apunten a desvincular a dicha persona del proceso penal en curso. Siendo así, deben evitarse cualesquiera juicios paralelos a la instrucción penal porque la investigación en curso puede determinar la exculpación o desvinculación respecto al proceso penal de la persona investigada. El secreto también protege el buen éxito de la investigación y esto es más palpable cuando el juez declara el secreto del sumario que afecta a las partes personadas, como se ha dicho, exceptuado el Ministerio Fiscal.
5. Me he ocupado de la relación justicia-medios de comunicación en dos ocasiones anteriores. Cito aquí las dos referencias en el entendido de que algunas de las afirmaciones que hago ahora tienen su sustento en ellas: Guzmán Fluja (1991, pág. 593-610), que pese al tiempo transcurrido mantiene una gran parte de su vigencia; donde ya analicé la cuestión de las filtraciones y la afectación de la presunción de inocencia por los juicios paralelos. El TEDH, por ejemplo, Sentencia de 17 de octubre de 2003, caso Craxi (2) v. Italia, a la vez que protege el secreto profesional del periodista, viene a establecer un deber del Estado de investigar eficazmente las filtraciones judiciales; véase al respecto Bustos Gilabert (2017).



Con independencia del resultado final, condenatorio o no, del proceso penal sobre el que se informa, hasta llegar a ese resultado por la vía de los juicios paralelos se habrán socavado muchos otros derechos fundamentales, como el honor, la intimidad, la propia imagen, la presunción de inocencia, que tendrán muy difícil reparación; se habrán generado penas añadidas a las que el ordenamiento jurídico establece para el caso de condena, como por ejemplo la llamada «pena de banquillo», o la recuperación «social» de penas medievales e inquisitoriales como la vergüenza pública o escarnio. Y si esto es intolerable incluso en caso de condena, mucho más en caso de absolución o cuando esas otras penas se aplican mediante el juicio paralelo que se forma a lo largo de la instrucción penal, cuando todavía rige en todo su esplendor la presunción de inocencia. Todo esto se ha visto agravado, muchas veces de forma extrema, por la irrupción de las redes sociales.

## 2. Las redes sociales como elemento de amplificación y mayor distorsión de los juicios paralelos

Las redes sociales no son sino un paso más en el fenómeno de los medios de comunicación masivos. Que un proceso penal sea noticia y, por ello, se informe (y en su caso, se opine) sobre su devenir y resultado ha sido algo común desde que hay medios de comunicación. Que el alcance e impacto de esa información en la generación de estados de opinión pública ha aumentado con el paso del tiempo es algo obvio por la propia evolución de los medios de comunicación, cada vez más masivos, de forma que el alcance

de las informaciones sobre los procesos penales pasa de un pequeño círculo de personas a potencialmente millones de ellas y el efecto perverso del juicio paralelo se extiende igualmente.<sup>6</sup> El efecto multiplicador de internet y de las redes sociales culmina, por el momento, esta evolución, en un doble sentido: los periodistas se sirven de las redes sociales para transmitir información de la manera más rápida y directa posible; a partir de ahí, los usuarios de las redes sociales interaccionan ante la información (que puede ser también que, de forma excepcional, no tenga origen periodístico) y empiezan a crearse corrientes de información y, sobre todo opinión, con un efecto multiplicador muy elevado.<sup>7</sup> Es imposible perder de vista el hecho de que los medios de comunicación son una potente fuente de alimentación e interrelación con las redes sociales.<sup>8</sup> En este sentido, ante un hecho criminal que se considere noticiable y objeto de información, el caso más preocupante no es el que se refiere a informaciones puntuales sobre el caso, sino aquel, cada vez más frecuente, en el que la libertad de información se pervierte para convertir el hecho criminal en tema central diario (hasta que se agote el tema o la audiencia) que ocupa los noticiarios de los distintos medios de comunicación, pero también muchos programas de radio y televisión, muchas páginas de medios escritos, muchos programas especiales sobre el caso, todo lo que es una potente fuente de alimento de las redes sociales. En muchas ocasiones, en estos programas, prima cualquier cosa que sirva para retener o aumentar la audiencia, a costa de la propia investigación criminal, a costa de los derechos de las personas relacionadas con el caso.

La principal dificultad para encontrar soluciones efectivas a la relación justicia-medios de comunicación estriba

- 
6. Es lo que pasa, por ejemplo, con la retransmisión de juicios por televisión. Se ha destacado que la presencia de medios de comunicación en la sala de vistas durante el juicio oral puede, además, suponer una alteración de comportamiento de los sujetos que intervienen en el mismo, desde el acusado a los testigos pasando por los jueces, sobre todo si son legos, llegando esto a ser expuesto por el TC alemán en una sentencia de 24 de enero de 2001, véase Montalvo Albiolop. *cit.*, pág. 120-121. Estos riesgos ya habían sido advertidos por Gerbner (1995a y 1995b, pág. 562-568). Una visión más positiva, desde un estudio de derecho comparado, en Ho Youm (2012, pág. 1.989-2.032). El autor sostiene que la actual prohibición de entrada de cámaras de televisión en la Supreme US Court (a diferencia de lo que sucede en las Cortes Supremas de Canadá, Reino Unido o Brasil, por ejemplo) será levantada tarde o temprano a la luz de la positiva experiencia de estas últimas. En España, véase la STC 57/2004, de 19 de abril, que considera no ajustado a derecho el Acuerdo de la Sala de Gobierno del Tribunal Supremo de 25 de septiembre de 1995, y el Acuerdo del CGPJ de 7 de febrero de 1996, en lo que respecta a la prohibición general de acceso de medios de comunicación al Palacio del Tribunal Supremo, acceso que debe ser autorizado caso por caso concreto. Desde otra perspectiva, resulta interesante consultar Orenes Ruiz (2014, pág. 121-140).
  7. Una aproximación muy ilustrativa en Azurmendi (2014, pág. 37-62).
  8. De nuevo, una aproximación al uso por los periodistas de las redes sociales para dar noticias inmediatas sobre lo que sucede en juicio, y sobre la interrelación de un medios de comunicación de masas, como la televisión, con las redes sociales, Azurmendi (*op. cit.*, pág. 54-58). La autora analiza en concreto esta interrelación al hilo del caso «Oscar Pistorius».

en que estamos ante una relación compleja y cambiante.<sup>9</sup> La libertad de información sobre procesos penales comienza a tratarse desde su posible colisión con los derechos al honor, la intimidad y la propia imagen de los acusados, así como desde la perspectiva de la influencia de las informaciones/opiniones en la imparcialidad de jueces profesionales y, en mayor medida, de los jueces legos o jurados; el panorama se ha ido complicando con el fenómeno incomprensiblemente asumido de las filtraciones, lo que pone bajo la lupa del juicio paralelo al personal al servicio de la justicia, a los propios abogados, a la vez que se extiende a los testigos y de los informes técnicos sobre pruebas materiales. También se produce una excesiva exposición mediática de las víctimas, caso en que hay que tener en cuenta si se trata de víctimas especialmente vulnerables como pueden ser los menores de edad, las mujeres víctimas de violencia de género, entre otras; a la vez se empieza a poner en riesgo el derecho a la presunción de inocencia de los investigados/acusados considerando dicho derecho desde una perspectiva extrajurídica.

El último cambio aludido, la generalización del uso de las redes sociales, contribuye fuertemente a amplificar los efectos de la información/opinión sobre la justicia, y distorsiona en gran medida la relación información-justicia penal, acentuando los males de los juicios paralelos. Constatado que los profesionales de la información se sirven de las redes sociales para su trabajo informativo y/o de opinión (es habitual que los periodistas que siguen los juicios en la sala de vistas estén tuiteando lo que sucede en ella), las redes sociales aportan un factor nuevo: cualquier persona, incluso los no profesionales de la información, los que no pertenecen ni trabajan para ningún medio de comunicación, puede intervenir ampliamente informando y opinando sobre un proceso penal en curso. El público se erige, a su vez, en informador y, sobre todo, opina, aspira a crear opinión (vertiente pasiva de la libertad de información deformada). Y entre los usuarios de las redes sociales deben tener especial mención los profesionales del sector legal cuyas informaciones, opiniones, comentarios o puntualizaciones sobre el caso

penal concreto objeto de juicio paralelo pueden tener una mayor influencia sobre los demás usuarios de las redes sociales.<sup>10</sup>

Las redes sociales, dentro de esa variedad de características propias de cada una que dijimos antes, hacen más peligrosos los juicios paralelos desde el momento en que se puede actuar desde el anonimato, pueden provocar una alta viralidad (expansión o extensión muy rápida y muy amplia) de la información u opinión sobre el proceso penal y sus partícipes, puede ocurrir que el tema interese a usuarios que tienen una posición dominante de sus perfiles de redes sociales (los llamados *influencers*, que tienen un gran número de seguidores y que con sus comentarios generan auténticas tendencias de opinión). Asimismo, las redes sociales contribuyen a la creación de estados de opinión confrontados sobre un mismo caso judicial (defensores contra detractores de los investigados, los testigos, las víctimas, la forma de efectuar la investigación, etc.), estados que pueden ser exacerbados. Y muy importante, aunque sobre esto volveremos luego, es que la gran mayoría de los usuarios que contribuyen a la génesis y mantenimiento del juicio paralelo no son profesionales, ni de la información, ni de la comunicación, ni de la justicia, por lo que expresan más bien opiniones basadas en su creencia de cómo deben ser las cosas.

Con todos los factores descritos en este apartado, se debe reconocer que la combinación es, desde luego, explosiva. Durante un período de tiempo, más o menos prolongado, un caso penal será eje de muchos programas en los diversos medios de comunicación, será objeto de tratamiento en las redes sociales, será un caldo de cultivo que alimentará el juicio paralelo. A veces todo termina abruptamente, porque ya no interesa y no genera beneficios o audiencia, a veces todo cesa para volver a empezar en cuanto alguna noticia sobre el caso sirva para revivirlo y volver a generar audiencias y beneficios.

Si nos centramos en el momento del juicio oral y de la posterior decisión del caso penal, la cuestión es saber si los juicios paralelos alimentados por las redes sociales

9. Y también en la falta de una actuación más decidida del legislador español. En otros países se han hecho reformas legales que endurecen las sanciones económicas y penales a quienes generan juicios paralelos; puede verse en extenso en Ovejero Puente (2017) y dentro de él en concreto Lecucq (2017). Sobre estos avances en Francia y Alemania, puede verse también Ovejero Puente (2017, pág. 431-455).

10. Como se comentó antes, las relaciones entre las redes sociales y el mundo jurídico en general, y el procesal en particular, son muy amplias. Una visión general sobre estas relaciones en Elliott Vinson (2010, pág. 356-413).

añaden algo nuevo a la posible influencia en el transcurso del juicio y en esa decisión final.<sup>11</sup> En este sentido, los jueces profesionales tienen un mayor blindaje ante la influencia de los juicios paralelos, antes y después de las redes sociales, sin descartar que puntualmente estos puedan afectar a la imparcialidad de la decisión, aunque es ciertamente infrecuente. Pero mucho más delicado es el tema cuando se trata de jurados o jueces legos a quienes los juicios paralelos pueden influir mucho más en su decisión. Aquí, las redes sociales aportan algo más a la posible influencia del «trial by press» sobre los jurados, sobre todo si estos mantienen un abierto contacto con las redes sociales durante la tramitación del juicio oral.<sup>12</sup> Esto va mucho más allá de una cuestión teórica y se han dado ya varios casos prácticos en otros países sobre la forma en la que se produce esta influencia y, de qué manera puede solucionarse.<sup>13</sup>

### 3. Redes sociales y derechos al honor, la intimidad y la propia imagen

Es sabido de sobras que el ejercicio del fundamental derecho a la libertad de información, unido o no al de libertad de opinión, provoca colisiones de mayor o menor gravedad con otros derechos fundamentales, sobre todo con los derechos al honor, a la intimidad y a la propia imagen. Hay tanto una abundante y consolidada doctrina del Tribunal Constitucional como jurisprudencia del Tribunal Supremo que han establecido las reglas y condiciones en las que la libertad de información prevalece sobre los otros derechos fundamentales.<sup>14</sup> Cabe decir que esta prevalencia de la libertad de información es la regla general que solo cede en concretos casos, regla que está en consonancia con la línea marcada por el Tribunal Europeo de Derechos Humanos.<sup>15</sup>

Si se trata de ejercicios de la libertad informativa, que inciden sobre el honor, la intimidad o la propia imagen de personas que están relacionadas con un proceso judicial en curso, las anteriores reglas y condiciones deben servir, en principio, para determinar qué derecho fundamental

11. Estamos ante un problema que afecta a derechos fundamentales como el honor, la intimidad, la propia imagen, incluso la presunción de inocencia, el proceso debido (no afectación de la imparcialidad), que se condensa en la doctrina USA en no afectar al derecho del acusado a un juicio justo. No regular adecuadamente el acceso y uso de las redes sociales durante el juicio supone un riesgo de convertir al propio tribunal en un «twitter»; véase Janoski-Haehlen (2011, pág. 43-68). La autora, partiendo del grave impacto que el uso de las redes sociales, sobre todo Twitter, puede tener sobre jueces, jurados y otros partícipes en el juicio oral hasta afectar al derecho a un juicio justo que tiene el acusado, propone determinadas soluciones que se resumen en medidas preventivas de carácter ético para jueces y medios de comunicación o un sistema más claro de advertencias a los jurados sobre el no uso de las redes sociales, hasta medidas sancionadoras efectivas en dinero o en medias administrativas o penales suficientemente disuasorias, pasando por una implicación mayor de los responsables de las redes sociales a la hora de prevenir y sancionar las conductas por uso de las redes sociales que ponen en riesgo el desarrollo del juicio conforme al «fair trial». Los tribunales, estatales o federales, deben también establecer reglas claras sobre los límites en que es admisible usar redes sociales durante los juicios.
12. Azurmendi (*op. cit.*, pág. 40-42), analiza las dos primeras sentencias condenatorias por el uso de redes sociales durante un juicio en el Reino Unido: en un primer caso se demostró que, durante el desarrollo del juicio, una de las jurados, actuando bajo pseudónimo, estuvo en contacto con la acusada a través de Facebook, y discutieron sobre el caso cuando el jurado aún deliberaba, por lo que incurrió en desacato; en el segundo caso, una miembro del jurado vulneró la prohibición expresa de consultar internet durante el juicio, de forma que buscó información sobre el caso y la compartió con el resto de los jurados, siendo condenada a seis meses de prisión.
13. Simpler III (2012, pág. 275-296), donde analiza una doble perspectiva del problema que implica una seria amenaza al derecho del acusado a un juicio justo y a ser juzgado por un jurado imparcial: 1) durante las sesiones del juicio, los jurados consultan internet y las redes sociales para disponer de fuentes de información que les ayuden en las deliberaciones y en la decisión, y 2) los jurados comparten en las redes sociales sus percepciones y opiniones de lo que está pasando en el juicio. Véase también Marder (2014, pág. 617-668).
14. Entre muchas otras, SSTC 76/2002 de 8 de abril, 139/2007 de 4 de junio, STC 56/2008 de 14 de abril, 68/2008 de 24 de julio, 29/2009 de 26 de enero; SSTS Sala 1.ª 199/2009 de 18 de febrero, 400/2009, de 12 junio, 718/2010 de 26 de octubre, 24/2015, de 29 enero, 269/2015, de 19 de mayo.
15. La doctrina del TEDH al respecto, con los criterios de ponderación y las matizaciones aplicables, se resume con mucha claridad en la STEDH Couderc et Hachette Filipacchi Associés v. Francia de 10 de noviembre de 2015.

debe prevalecer en el caso concreto.<sup>16</sup> Centrándonos en el sujeto investigado-acusado, a quien el juicio paralelo «mediático» surgido al hilo del proceso judicial en sus diversas fases afecta principalmente, los posibles ataques a su honor, intimidad, propia imagen lo serán en cuanto presunto partícipe en la comisión de un hecho delictivo, y esos ataques están dirigidos a sembrar en la opinión pública la idea de que efectivamente tiene relación con la comisión del delito o que su trayectoria vital, también sometida a escrutinio, apunta a que es una persona que ya ha mostrado conductas sospechosas o que su comportamiento es moral y/o socialmente reprochable. Así, el investigado-acusado corre el riesgo de un doble daño en forma de doble condena, social-mediática y jurídica.

En este escenario, las redes sociales suponen, como se viene sosteniendo, un agravamiento de las consecuencias lesivas del juicio paralelo sobre el honor, intimidad o propia imagen de las personas relacionadas con el proceso penal. Y supone la aparición de factores que hacen inaplicable la doctrina jurisprudencial antes citada.

En efecto, para ambos tribunales la libertad de información es un derecho que tiene primacía sobre el derecho al honor, a la intimidad y a la propia imagen, sobre la base de que la información es proporcionada por un medio de comunicación, y dentro de él por un profesional de la información, y tiene la característica de ser objetiva y veraz. Asimismo, son factores importantes la relevancia de la información para la formación de la opinión pública, el carácter público del sujeto afectado (las personas con relevancia pública deben soportar un riesgo mayor de lesión de sus derechos como consecuencia del ejercicio de la libertad de información) y la forma de presentar la información que no debe ser sesgada, ni difamatoria, ni tener propósito de descalificación o descrédito.<sup>17</sup> Cuando trasladamos esa doctrina a la relación medios de comunicación-justicia, en principio cabría decir que un proceso penal, en cualquiera

de sus fases pero sin duda en el juicio oral, puede ser objeto de información como ya hemos dicho. Cumpliéndose estas condiciones fijadas por la jurisprudencia, la libertad de información debe prevalecer, pero esto no exime a los medios de comunicación, y a los informadores, de evitar que la información vaya acompañada de valoraciones que tergiversen o sesguen lo que está sucediendo en el juicio oral o que se excedan al incluir comentarios sobre las personas que intervienen en él para anticipar el resultado del proceso en un concreto sentido. Es decir, la libertad de información no debe generar juicios paralelos.

En el caso de la fase de instrucción, el problema es distinto. Partiendo de que lo que sucede en esta fase debe ser secreto para los terceros, incluidos los medios de comunicación, la Administración de Justicia debe ser la que determine qué información, y bajo qué condiciones, se debe proporcionar para cumplir con el respeto a la libertad de información sobre un caso que se está investigando. Debe haber un control sobre esa información. Pero es sabido que esto no es así y que, en los casos más relevantes desde el punto de vista informativo, el secreto de las actuaciones sumariales es una quimera desde el momento en que prácticamente cualquier actuación de la instrucción se hace pública, muchas veces de forma inmediata a haber sucedido (por ejemplo, es habitual que una declaración de un investigado se haga pública nada más este sale de las puertas de juzgado en el que acaba de declarar). Aunque no se haya puesto solución a esta tremenda situación, más allá de comportamientos éticos asumidos por algunos medios de comunicación y periodistas, lo cierto es que todas estas filtraciones, pues no otro es el problema, son ilegales y tienen su respuesta por la vía disciplinaria, la vía civil y la vía penal (tanto para funcionarios de la Administración de Justicia como para abogados o cualquier otra persona que tiene conocimiento de las actuaciones instructoras y no respeta la debida confidencialidad), pero no se han activado hasta

- 
16. Y así, por ejemplo, se afirma en la STC 6/1996, de 16 de enero, referida a informaciones que relacionan a una persona con la comisión de determinados hechos delictivos, que la protección que dispensa el artículo 21.1.d) CE se extiende solo a la información veraz, entendida no como verdad objetiva e incontestable, sino como especial diligencia en la búsqueda de lo cierto o en contrastar debidamente la información, evitando transmitir rumores, invenciones, insinuaciones, visiones parciales, segadas o mendaces del caso. Todo ello, en el caso, implicó una ilegítima intromisión en el honor del afectado.
17. Las condiciones de primacía de la libertad de información no funcionan exactamente igual respecto de los tres derechos fundamentales citados: por ejemplo, la condición de veracidad ampara la libertad de información sobre el derecho al honor, pero no frente al derecho a la intimidad. En extenso, con examen de la última jurisprudencia, pueden verse todas estas cuestiones en Madrona Ortega (2018). También es bastante interesante el análisis de Carrillo (2017).

el momento que se sepa. Y tampoco ayuda la fuerza con la que opera el derecho que tienen los periodistas a no revelar sus fuentes de información. El caldo de cultivo para la aparición de juicios paralelos es muy amplio y esto no tiene justificación desde el momento en que se generan a partir de informaciones que, más allá de lo que sería acorde con la ley, no deberían ser de conocimiento público y no deberían estar amparadas por el ejercicio de la libertad de información. A partir de ahí, las lesiones de derechos fundamentales que se produzcan deberían encontrar amparo por encima del derecho a informar, por muy objetiva y veraz que sea la información, porque se sustenta en informaciones que están cubiertas por un secreto legal configurado en la LECrim.

Con las redes sociales, en el escenario descrito, lo que sucede es que encontramos diversas situaciones. En primer lugar, si se usan como un instrumento más por parte de medios de comunicación y profesionales de la información, lo dicho antes sería de plena aplicación, dado que la red social no sería más que un instrumento más del que se sirve el medio de comunicación para dar información acompañada o no de opinión. Si se trata de profesionales de la justicia que usan las redes sociales para comentar un caso, estarán sujetos, por la misma razón, a sus códigos profesionales y a la aplicación, en su caso de las leyes disciplinarias, civiles o penales cuando vulneren derechos fundamentales.

Pero, en segundo lugar, hay un enorme número de usuarios de las redes sociales que no son profesionales, ni de la información ni jurídicos, y por ello no están sometidos a códigos deontológicos ni a responsabilidades disciplinarias. Desde luego, no son profesionales de la información y no están cubiertos, por ello, por la ya expuesta doctrina de los tribunales dado que esta opera solo respecto de medios de comunicación y profesionales de la información.<sup>18</sup> Para estos casos, la única vía, además de las medidas que pueda tomar la red social por mal uso de la misma (y la responsabilidad en que pueda incurrir por no tomarlas), es la presentación de demandas civiles o, en su caso acudir a la vía penal, cuando los comentarios vertidos lesionen los derechos de las personas relacionadas

con el caso penal objeto de información. Esta tarea puede estar dificultada por algunas de esas características de anonimato, alta viralidad (un gran número de posibles infractores).

En resumen, los usuarios no profesionales de la información (o jurídicos) de las redes sociales no entrarían dentro del ámbito subjetivo de aplicación de la doctrina judicial que hace prevalecer la libertad de información sobre otros derechos. Es urgente legislar de forma más concreta qué medidas específicas, más allá de las respuestas por vía civil y penal, se deben adoptar para garantizar que los excesos de las redes sociales traducidos en vulneraciones de derechos no quedan impunes.

#### 4. Redes sociales y presunción de inocencia

La constatación de que los juicios paralelos podían dar lugar a una afectación de la presunción de inocencia se integra en la «historia contemporánea» de la relación justicia-medios de comunicación, siendo objeto de una importante preocupación doctrinal.

El derecho fundamental a la presunción de inocencia protege exclusivamente al sujeto pasivo del proceso penal en sus diversas fases, no a otros sujetos. Y opera como concepto jurídico, que es su sentido prístino, dentro de un proceso penal dirigido contra una persona concreta que, durante la tramitación del proceso penal en cualquiera de sus fases, tiene el derecho a ser considerada inocente hasta que no haya una sentencia firme de condena en su contra. La pregunta es, dado que el derecho fundamental solo opera en un campo de juego jurídico, si los juicios paralelos, y las redes sociales que los alimentan, pueden menoscabarlo.<sup>19</sup>

La existencia de un juicio paralelo, propiciado por los medios de comunicación y las redes sociales, debe proyectarse, pues, en un resultado dentro del proceso penal para entender que ha producido un efecto negativo sobre la

18. Sobre estas cuestiones, véase Madrona Ortega, *op. cit.*

19. Es muy extensa la doctrina sobre la presunción de inocencia. Un acertado corolario de su evolución como derecho fundamental, además reciente, en Ovejero Puente (*op. cit.*, pág. 431-437).



presunción de inocencia<sup>20</sup> contribuyendo a que sea enervada de manera injustificada y conduciendo a un resultado diferente (la condena, o una condena más grave) del que se habría dado (absolución o una condena más leve) de no haberse producido esa influencia del juicio paralelo en la sentencia, en la decisión judicial, influencia que habrá supuesto, además, una afectación de la imparcialidad del juzgador. La doctrina jurisprudencial consolidada,<sup>21</sup> a este último respecto, es que debe probarse en el caso concreto que un juicio paralelo ha producido una alteración indebida de la imparcialidad del juzgador en la decisión del caso.<sup>22</sup> De no ser así, el juicio paralelo mediático y de las redes sociales no queda sino en un ruido, más o menos importante, que acompaña al juicio penal, enturbiando su entorno, pero que no le afecta en su resultado, de forma que si la decisión de condena, o de condena más grave, es ajena a ese ruido y se ha tomado sobre la base de los factores estrictamente jurídicos y fácticos producidos en el juicio oral, el juicio paralelo, incluida la contribución al mismo de las redes sociales, no habrá afectado a la presunción de inocencia (aunque puede que a otros derechos fundamentales, como hemos visto más arriba).<sup>23</sup> Siendo así, lo que quedaría es ver si el juicio paralelo puede suponer una afectación extraprocesal de la presunción de inocencia.

Determinar si la presunción de inocencia tiene una vertiente social, extraprocesal o extrajurídica es un tema complejo, pero parece abrirse paso la respuesta positiva. Doctrina y jurisprudencia apuntan a que existe, y cada vez con más fuerza, esta vertiente social de la presunción de inocencia, que los juicios paralelos mediáticos pueden afectarla, y que las redes sociales son un instrumento especialmente dañino en este sentido. Se admite sin debate que esta dimensión extraprocesal vincula a todas las autoridades públicas (no sólo judiciales) que deban facilitar información a los medios de comunicación y a la sociedad sobre un hecho delictivo y su posible partícipe,<sup>24</sup> y así lo establece la Directiva 2016/343, del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio.<sup>25</sup>

Compartiendo lo anterior, es necesario ampliar el ámbito extraprocesal de la presunción de inocencia para proteger este derecho, y a sus titulares, de las vulneraciones que puedan sufrir vía juicios paralelos que pueden generar estados de opinión pública deformes que hagan percibir como culpable a quien todavía no lo es, ni siquiera es se-

20. Mientras el juicio mediático se mantenga «paralelo» al juicio judicial, aquel no influirá en el resultado de este (lo que no evita que sea dañino). El problema aumenta cuando el juicio mediático deja ser «paralelo» al judicial y se convierte en «oblicuo» o «perpendicular» respecto a este. De juicio «perpendicular» habla Chaves (2018); la expresión juicio «oblicuo», como aquel mediático que influye en la sentencia, la ha empleado el magistrado del Tribunal Supremo Antonio del Moral, según noticia recogida en <<https://conflegal.com/20150611-magistrado-antonio-moral-distingue-juicios-paralelos-oblicuos-10062015-1716/>>.
21. Citando la doctrina del TC y la jurisprudencia del TS, véase la STS, Sala Penal, 875/2016 de 21 de noviembre de 2016, que añade que esta posición es también aplicable a los jurados, por más que suela afirmarse que resultan más vulnerables a la presión mediática. La Sentencia Tourancheau y July v. Francia, de 24 de noviembre de 2005 (definitiva de 12 de abril de 2006), ha señalado que la opinión mayoritaria de la doctrina considera que los jurados, por su ausencia de entrenamiento, menor cultura jurídica y mayor proximidad con la comunidad, son especialmente sensibles a las presiones mediáticas, lo que justifica su especial protección; así, este tribunal entiende que los jurados son más influenciados por la presión mediática que los jueces profesionales, véase Bustos Gilabert, *op. cit.*
22. Véase Valldecabres Ortiz (2004); puede verse también Barrero Ortega (2010, pág. 193-207). Es decir, la imparcialidad se presume y su pérdida debe ser probada, entre otras, STC 140/2004, de 13 de septiembre, STS 72/2011, Sala 2.ª, de 15 de febrero de 2011; STSJ Galicia 2/2016, de 15 de marzo.
23. Nótese que nos centramos en el juicio oral y en la decisión final del caso. Pero la presunción de inocencia es un derecho fundamental que exige respeto a lo largo de toda la tramitación del proceso penal. Todas las actuaciones procesales, policiales, fiscales, judiciales, de parte, y todas las decisiones de los tribunales deben hacerse observando siempre la necesidad de hacerlas compatibles con el respeto a la presunción de inocencia en atención a la actuación de que se trata y al momento procesal en que se lleva a cabo. Pese a ello, algunas actuaciones y decisiones suponen un legítimo desgaste de la presunción de inocencia (detención, prisión provisional, procesamiento, apertura del juicio oral), justificado en la necesidad de investigar y resolver el caso penal adoptando las medidas necesarias, conforme a los datos disponibles en cada momento, para hacer posible el más correcto avance del proceso penal. Pero no se olvide que estas otras decisiones no deberían verse influidas por un juicio paralelo, ni por las redes sociales que lo alimentan, sobre todo porque no deberían producirse bajo ningún concepto en la fase de instrucción.
24. Así lo establece el TEDH en una línea jurisprudencial consolidada desde la sentencia *Allenet de Ribemont v. Francia*, de 10 de febrero de 1995, véase un análisis en Bustos Gilabert, *op. cit.*
25. Un comentario más extenso sobre la directiva en Ovejero Puente (*op. cit.*, pág. 449-454).



guro que lo sea o lo termine siendo. Y, por lo tanto, los medios de comunicación y las redes sociales deben ser también respetuosos con la presunción de inocencia única, solución congruente con el respeto razonable a esta vertiente extraprocesal. Ahora bien, es cierto que esta vertiente extraprocesal no alcanza entidad como derecho fundamental autónomo, pero eso no debe significar que su lesión quede reducida a una mera subsunción en la lesión de otro derecho fundamental, como puede ser el derecho al honor, a la intimidad o la propia imagen.<sup>26</sup> Si un juicio paralelo propicia que se cree una apariencia de culpabilidad respecto de un investigado-acusado, cierto que se lesiona su honor, y que ahí hay una vía de reacción, pero también es cierto que se le provoca un daño añadido consistente considerarlo anticipadamente, y de forma injustificada, como delincuente no en abstracto sino en relación con un concreto hecho delictivo objeto de un proceso penal en curso.<sup>27</sup>

De nuevo, diferenciamos: 1) en el juicio oral, los medios de comunicación y las redes sociales deben informar y comentar ateniéndose estrictamente a lo que sucede en el mismo de forma objetiva y veraz, sin hacer interpretaciones que adelanten un resultado final condenatorio porque, si finalmente hay condena, esta no se puede anticipar socialmente, no es tolerable que así sea, y si finalmente hay absolución, el daño de haber sido considerado socialmente culpable va a quedar como «pena social» difícil de borrar (además de poder generar la sensación de que la justicia se ha equivocado); 2) en la fase de instrucción, partiendo del absoluto irrespeto que hay hacia el secreto del sumario, medios de comunicación y redes sociales suelen afanarse en retransmitir, casi en vivo y en directo, toda la investi-

gación de manera que, a medida que las investigaciones van esclareciendo los hechos, se transmite, de forma más o menos velada (y con el manido «presunto» por delante), que todo apunta hacia la culpabilidad del investigado, y se genera la creencia social de que es efectivamente culpable, así como la expectativa de que será condenado, y este estigma social quedará con independencia del resultado final.

Con todo, hay que reconocer que es muy difícil poner freno a la vulneración de la vertiente extraprocesal de la presunción de inocencia por los juicios paralelos, todavía más por las redes sociales que participan de ellos. El TEDH no ha dado el paso de colocar a los medios de comunicación<sup>28</sup> en cuanto generadores de juicios paralelos, como sujetos que puedan infringir la presunción de inocencia en su vertiente social (pero también es cierto que les impone ciertas obligaciones para un ejercicio legítimo de la libertad de información, por ejemplo, cumplir con las normas y con los códigos deontológicos, que por cierto suelen establecer como regla de conducta el respetar la presunción de inocencia a la hora de informar sobre casos penales, informar sobre una base fáctica suficiente, hacer cometarios leales, etc.),<sup>29</sup> lo cual es también aplicable a los particulares que usan las redes sociales y contribuyen a esos juicios mediáticos. En España podría argüirse que los particulares, incluidos los medios de comunicación privados, pueden vulnerar derechos fundamentales a otros particulares (base de la aplicación en nuestro país de la teoría de la prueba ilícita desde la STC 114/1984, de 29 de noviembre); pero esto sería posible respecto de los derechos fundamentales materiales, no respecto de los derechos fundamentales procesales, como la presunción de inocencia.

26. Sobre esta teoría, que goza de predicamento en buena parte de la doctrina, véase en extenso Camarena Aliaga (2017, pág. 185-197). Partidaria de un avance mayor de esta perspectiva extraprocesal de la presunción de inocencia, Ovejero Puente (*op. cit.*, pág. 454-455).
27. Por ejemplo, afirmar que X es un ladrón o un corrupto, sin que se haya abierto ningún proceso penal al respecto, es considerar a X un posible delincuente en abstracto, algo que sin duda puede lesionar su honor, pero en ningún caso la presunción de inocencia en vertiente extraprocesal. Alguna diferencia tiene que haber si tales afirmaciones se efectúan habiendo un proceso penal abierto por robo, hurto o corrupción, porque, además de la posible lesión del honor, se le estaría haciendo culpable de esos delitos concretos sin que ninguna sentencia haya establecido esa culpabilidad.
28. SSTEDH Worm v. Austria, de 29 de agosto de 1997; Tourancheau y July v. Francia, de 24 de noviembre de 2005 (definitiva de 12 de abril de 2006), y Dámaso Campos v. Portugal, de 24 de abril de 2008, entre otras. Véase Bustos Gilabert, *op. cit.* Igualmente, una excelente exposición y valoración de la doctrina del TEDH en Ovejero Puente (*op. cit.*, pág. 443-448), donde señala que el TEDH, como se deduce de las sentencias antes citadas, ha optado por subsumir la afectación de la presunción de inocencia dentro de la posible vulneración del derecho a un juicio justo.
29. SSTEDH Du Roy & Malaurie v. Francia, de 3 de octubre de 2000; Goodwin v. Reino Unido, de 11 de julio de 2002; Craxi (2) v. Italia (2002); Stoll v. Suiza, de 10 de diciembre de 2007; Voskuil v. Holanda, de 27 de noviembre de 2007; y Gutsanovi v. Bulgaria de 15 de octubre de 2013, entre otras. De nuevo, puede verse con detalle esta doctrina en Bustos Gilabert, *op. cit.*, y Ovejero Puente (*op. cit.*, pág. 443-448).

Los juicios paralelos, y su amplificación vía redes sociales, puede suponer que medios de comunicación y usuarios de las mismas terminen creando estados de opinión pública que presenten como culpable de un crimen a quien todavía no lo es legalmente, y para ello escudriñan hasta la náusea en la vida personal del investigado acusado para resaltar los aspectos que abonan esa culpabilidad. Aunque esto no tenga trascendencia jurídica, es una situación que el investigado-acusado no debería soportar de ninguna de las maneras (tampoco aunque finalmente el juez lo declare culpable), porque supone un estigma no justificado.

Cierto es que el afectado puede reaccionar contra el daño sufrido por la vía de reclamar por vulneración del derecho al honor, a la intimidad o a la propia imagen, pues con seguridad se habrán violentado para generar esa situación de culpabilidad ante la sociedad. Y ahí es posible actuar tanto contra el medio de comunicación, y el periodista concreto en su caso, como contra los usuarios de las redes sociales. Igualmente, cabe pedir que los responsables de la gestión de las redes sociales, de conformidad con sus condiciones de uso, extremen las medidas, tales como la suspensión de correspondiente cuenta, contra los usuarios que contribuyan a generar y alimentar juicios paralelos que hagan aparecer anticipadamente (y por ello indebidamente) como culpable al sujeto pasivo del proceso penal.

Pero, en mi opinión, las normas deberían ser modificadas para incluir como agravante en esas reclamaciones por vulneración del honor, la intimidad o la propia imagen el que se hayan producido por medio de un juicio paralelo que implica, también, la vulneración extraprocesal de la presunción de inocencia. Y esta agravante se aplicaría a medios de comunicación, periodistas concretos, en su caso, usuarios de las redes sociales, y debería tener su lugar también como causa específica de suspensión del uso de la correspondiente red social. Se trata de generar la conciencia social de que la presunción de inocencia es un valor esencial que se debe respetar en todos los ámbitos.

## 5. Conclusión

En realidad, la dimensión del problema derivado de la existencia de juicios paralelos es más cualitativa que cuantitativa. Teniendo en cuenta los cientos de miles de casos penales que se resuelven por sentencia en España en un año dado,<sup>30</sup> la inmensa mayoría de los mismos está fuera del foco informativo: o no son reseñados en modo alguno por los medios de comunicación, ni son objeto de seguimiento o tratamiento en las redes sociales, o por la concurrencia de un factor subjetivo (sea el acusado, sea la víctima) o de un factor objetivo especialmente llamativo (modo de comisión, por ejemplo) son noticiables en algún momento, inicial, intermedio o final, pero no tienen un seguimiento continuo capaz de generar un juicio paralelo.

La atención continua, a veces agotadoramente exhaustiva, de los medios de comunicación, y de las redes sociales, recae sobre un pequeño número de casos penales, los que se consideran más atractivos para generar audiencia. Por lo tanto, los juicios paralelos afectan a un número muy pequeño de casos penales. Esto no quita ni un ápice de importancia al problema, pero siempre es bueno tener claro que no estamos ante un problema general. Puede decirse, pues, que la magnitud del problema de las interferencias del juicio paralelo mediático con el juicio penal, así como de las confrontaciones entre derechos fundamentales, es escasa en términos cuantitativos, pero grande en términos cualitativos.

Las redes sociales contribuyen a magnificar los juicios paralelos y multiplican las eventuales lesiones de los derechos fundamentales que hemos visto en este trabajo, a la vez que elevan exponencialmente su difusión y conocimiento por los diversos estados de opinión pública. Es necesario prestar atención a esta situación porque, aunque el ordenamiento jurídico presenta instrumentos que pueden ser aptos para sancionar, civil o penalmente, a los autores de estas vulneraciones, no hay todavía elementos específicos que atiendan a la significación cualitativa y cuantitativa del daño que se causa a través de las redes

30. El estudio del CGPJ «La justicia dato a dato 2015» referencia que, en 2015, ingresaron en la jurisdicción penal 5.805.619 asuntos y se dictaron 644.693 sentencias; el mismo estudio para 2016, último disponible hasta la fecha, referencia que ingresaron 3.365.927 asuntos y se dictaron 644.693 (sí, curiosamente, la misma cifra que en 2015!). En realidad, se puede comprobar, anualmente se inician millones de procesos penales. Pero si nos referimos a los que son resueltos, esa cifra baja ostensiblemente hasta situarse en cientos de miles. Por supuesto, esta situación tiene explicación lógica que excede del propósito y extensión de estas líneas.

sociales. A ello debe unirse una consideración más específica de la protección de la vertiente social de la presunción de inocencia, sin que llegue a alcanzar la condición de derecho autónomo, pero dándole carácter de regla de tratamiento obligado para medios de comunicación y usuarios de redes sociales. Igualmente, se requiere una mayor implicación de los responsables de gestión y uso de las redes sociales para activar mecanismos preventivos y, en su caso, represivos, cuando se detecta que hay usuarios, que pueden ser cientos o miles, que usan sus cuentas para contribuir a expandir juicios paralelos que lesionan derechos fundamentales de quienes están implicados en el caso penal objeto de información. Un importante papel tendrá el auge del llamado «derecho al olvido» como mecanismo para borrar de medios de comunicación y redes sociales el rastro negativo causado por los juicios paralelos. Por último, se hacen necesarias medidas como la restricción del anonimato en las redes sociales,<sup>31</sup> un mayor control sobre los *bots* o cuentas automatizadas que replican información y opinión de forma masiva, así como sobre los *trolls* y un seguimiento más rígido de los usuarios con mayor capacidad de influencia y de creación de estados de opinión pública, dado que su responsabilidad a la hora de generar juicios paralelos y vulnerar derechos es mayor que la de otros usuarios.

## 6. Coda: dos ejemplos prácticos

Quiero terminar ofreciendo dos ejemplos de cómo las redes sociales hacen más invasivos los juicios paralelos generados por los medios de comunicación. Un primer ejemplo se centra en cómo pueden afectar a la víctima de un delito; un segundo ejemplo hace referencia a una persona investigada por un crimen.

En el caso conocido mediáticamente como el de «la manada», en referencia a la investigación y juicio por la violación múltiple de la primera noche de sanfermines de 2016, hemos asistido, en una conjunción de actos de la

defensa de los acusados, los medios de comunicación y las redes sociales, a la generación de varios juicios paralelos, muchos de ellos referidos a los acusados pero otros referidos... ¡a la víctima! Por supuesto, en un marco de informaciones que muchas veces carecían de objetividad y neutralidad, y de opiniones que sesgaban y tergiversaban la investigación y el juicio, de pronto la víctima de la agresión se ve sometida a un escudriñamiento absoluto de su vida, acentuado por el debate en las redes sociales, de sus comportamientos, de sus acciones, de su vida sexual, con la intención de crear opinión sobre sí, a la vista de esos antecedentes, pudo ser que más que una violación y se tratara de un acto consentido. Convengamos en que esto es intolerable, no es admisible en una sociedad moderna y democrática, y será muy difícil de reparar el daño causado a la víctima.

En los primeros meses de 2018, la desaparición de un niño de ocho años en Almería tiene el trágico desenlace de encontrar su cadáver en un vehículo conducido por su madrastra que, finalmente, a los dos días de ser detenida, confiesa ser autora del crimen. Medios de comunicación, programas de televisión casi monográficos, redes sociales hirviendo con diversos *trending topics* y *hashtags* sobre el suceso, además de contar al segundo el desarrollo de la investigación, sobre la base de las consabidas filtraciones (algo inexplicable), se dedicaron a analizar el perfil de la presunta autora del crimen (aunque confiesa, sabido es que la confesión, artículo 406 LECrim, no exime de la necesidad de instrucción judicial ni de abrir el correspondiente juicio oral, si hay elementos para ello, donde se dilucide definitivamente la autoría del delito), con opiniones sobre su personalidad, ilustradas por expertos en psicología, con una reconstrucción de su vida antes de la comisión del crimen en la que se deja entrever que ya era una persona problemática en su país de origen, situado en el Caribe. Esa personalidad problemática, con rasgos de frialdad y falta de empatía, se mantiene cuando llegó a España, con testimonios de vecinos, familiares de exparejas, que retratan, bajo una apariencia normal, a una persona aprovechada, que va dejando problemas por donde pasa.

31. Se requiere una mayor facilidad para averiguar quién está realmente tras una cuenta que funciona bajo anonimato o bajo pseudónimo, algo que actualmente es difícil y requiere una tarea investigadora importante, sobre todo si el usuario actúa desde un dispositivo situado fuera de España o a través de una plataforma que da servicio desde el extranjero. A finales de 2017, el Gobierno planteó la posibilidad de legislar para acabar con el anonimato en las redes sociales o restringirlo, lo que ha suscitado reacciones por la consecuente afectación de la libertad de expresión. En el mismo sentido se ha pronunciado el Fiscal General del Estado en marzo de 2018, mostrando, además, su preocupación por el uso del anonimato para generar situaciones de violencia contra la mujer.

Incluso se recuerda cómo una hija suya apareció muerta en el patio de la vivienda tras caer desde la ventana de un tercer piso (suceso que se investigó y se archivó, pero que ahora vuelve a levantar sospechas sobre qué ocurrió realmente). En definitiva, durante tres días se asistió a un auténtico linchamiento de esta persona propiciado por un juicio paralelo alimentado monstruosamente por medios de comunicación y redes sociales, todo ello dirigido a «justificar» que tiene que ser culpable. No es admisible que haya pasado esto, por mucho que haya confesado el crimen, porque solo tras la culminación de la investigación y solo tras el juicio oral habrá una sentencia en la que se determinen, conforme a derecho, los hechos criminales

y su autor. Hasta entonces, la libertad de información no puede amparar que se destroce moralmente a una persona investigada hasta el punto de convertirla casi en una persona ajena a la comunidad y por lo tanto merecedora de condena, de la condena más grave posible. La sentencia social ya está dictada, y aunque en su día la sentencia judicial sea coincidente, nadie, por muy investigado que sea, merece un trato tan denigrante como el que ha sufrido esta persona; sencillamente no es compatible con la protección ni con las garantías que dispensa el ordenamiento jurídico, en el Estado de derecho, a quienes son sospechosos de haber cometido un crimen.

## Bibliografía

- GOEZ, D. (2016). «Diferencias entre Facebook, Instagram y Twitter ¿Qué tipo de contenido es mejor para cada uno?». Juan Carlos Mejía Llano.com. [Fecha de consulta: 02/02/18] <<http://www.juancmejia.com/y-bloggers-invitados/facebook-twitter-e-instagram-que-tipo-de-contenido-es-mejor-para-cada-uno/>>
- MIRÓ LLINARES, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.
- BARRERA, S. (2017). *Claves de la investigación en redes sociales*. Editorial Círculo Rojo.
- MONTALVO ALBIOL, J. C. (2012). «Los juicios paralelos en el proceso penal: ¿anomalía democrática o mal necesario?». *Universitas. Revista de Filosofía, Derecho y Política*. N.º 16, pág. 105-110.
- GUZMÁN FLUJA, V. (1991). «Algunos aspectos de la relación justicia-medios de comunicación social». *Justicia: revista de derecho procesal*, n.º 3, pág. 593-610,
- GUZMÁN FLUJA, V. (2009). «Algunos apuntes sobre la responsabilidad estatal por funcionamiento de la justicia». *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, n.º 5, pág. 157-178.
- BUSTOS GILBERT, R. (2017). «Juicios paralelos y presunción de inocencia en la jurisprudencia del Tribunal Europeo de Derechos Humanos». En: A. M. OVEJERO PUENTE (ed.). *Presunción de inocencia y juicios paralelos en derecho comparado. III sesión del Observatorio de la presunción de inocencia y los juicios paralelos*. Tirant Lo Blanch.
- GERBNER, G. (1995). «Trial by Television: Are We at the Point of No Return». *Judicature*, n.º 9.
- GERBNER, G. (1995b). «Cameras on trial: the O.J. Show turns the tide». *Journal of Broadcasting and Electronic Media*, n.º 39, pág. 562-568.
- HO YOUM, K. 1989 (2012). «Cameras in the Courtroom in the Twenty-First Century: The U.S. Supreme Court Learning From Abroad?». *Brigham Young University Law Review*, pág. 1.989-2.032
- ORENES RUIZ, J. C. (2014). «El control no jurisdiccional de los juicios en televisión por parte de las autoridades audiovisuales». *Dilemata*, año 6, n.º 14, pág. 121-140.
- AZURMENDI, A. (2014). «Twitter en los juicios: una revolución en la información periodística de tribunales». *Correspondencias & Análisis*, n.º 4, pág. 37-62.

- OVEJERO PUENTE, A. M. (ed.) (2017). *Presunción de inocencia y juicios paralelos en derecho comparado. III sesión del Observatorio de la presunción de inocencia y los juicios paralelos*. Tirant lo Blanch.
- LECUCQ, O. (2017). «Presunción de inocencia y juicios paralelos en Francia». En: A. M. OVEJERO PUENTE (ed.). *Presunción de inocencia y juicios paralelos en derecho comparado. III sesión del Observatorio de la presunción de inocencia y los juicios paralelos*. Tirant lo Blanch.
- OVEJERO PUENTE, A. M. (2017). «Protección del derecho a la presunción de inocencia». *Teoría y Realidad Constitucional*, n.º 40, pág. 431-455.
- ELLIOTT VINSON, K. (2010). «The Blurred Boundaries of Social Networking in the Legal Field: Just Face it». *The University of Memphis Law Review*, vol. 41, pág. 356-413.
- JANOSKI-HAEHLEN, E. M. (2011). «The Courts Are All A 'Twitter': the Implications of Social Media Use in the Courts». *Valparaiso University Law Rev.* vol. 46, n.º 43, pág. 43-68.
- SIMPLER III, MILAND F. (2012). «The Unjust Web We Weave: The Evolution of Social Media and its Psychological Impact on Juror Impartiality and Fair Trials». *Law & Psychology Review*, n.º 36, pág. 275-296.
- MARDER, NANCY S. (2014). «Jurors and Social Media: Is a Fair Trial Still Possible?». *Southern Methodist University Law Review*, n.º 67, pág. 617-668.
- MADRONA ORTEGA, V. (2018). «La libertad de información frente a los derechos al honor, a la intimidad personal y familiar y a la propia imagen». *Proceso penal, presunción de inocencia y medios de comunicación*, Aranzadi (consultado, por gentileza de la autora, en las primeras pruebas de la publicación).
- CARRILLO, M. (2017). «Los juicios paralelos en derecho comparado: el caso de España». En: A. M. OVEJERO PUENTE (ed.). *Presunción de inocencia y juicios paralelos en derecho comparado. III sesión del Observatorio de la presunción de inocencia y los juicios paralelos*, Tirant Lo Blanch, 2017.
- CHAVES, J. R. (2018). «Presunción de inocencia ante Juicios paralelos y Juicios perpendiculares». *delajusticia.com*, el Rincón Jurídico de José R. Chaves. <<https://delajusticia.com/2018/01/26/presuncion-de-inocencia-ante-juicios-paralelos-y-juicios-perpendiculares/>>
- VALLDECABRES ORTIZ, M. I. (2004). *Imparcialidad del juez y medios de comunicación*. Tirant Lo Blanch, 2004.
- BARRERO ORTEGA, A. (2010). «La imparcialidad e independencia judicial frente a los medios de comunicación». *Revista do Tribunal Regional do Trabalho da 15ª Região*, n.º 36, pág. 193-207.
- CAMARENA ALIAGA, G. W. (2017). *Medios de comunicación y Poder Judicial: tratamiento procesal y penal frente a los juicios paralelos*, tesis doctoral, Universidad Autónoma de Madrid, Facultad de Derecho, pág. 185-197. <<https://repositorio.uam.es/handle/10486/680884>>

### Cita recomendada

Guzmán Fluja, Vicente C. (2018). «Juicios paralelos en las redes sociales y proceso penal». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 52-66. UOC [Fecha de consulta: dd/mm/aa]  
 <<http://dx.doi.org/10.7238/idp.v0i27.3148>>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre el autor

Vicente C. Guzmán Fluja  
 vguzflu@upo.es

Catedrático de Derecho Procesal  
 Universidad Pablo Olavide  
<https://www.upo.es/rectorado/rector/>

Universidad Pablo de Olavide, de Sevilla  
 Rectorado / Consejo de Dirección  
 Ctra. de Utrera, km. 1  
 41013 Sevilla



www.uoc.edu/idp

**Dossier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»**

ARTÍCULO

# Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre\*

Teresa Armenta Deu  
 Universitat de Girona

Fecha de presentación: mayo de 2018

Fecha de aceptación: julio de 2018

Fecha de publicación: septiembre de 2018

## Resumen

Este estudio se centra en los medios tecnológicos como fuente de investigación en el proceso penal y, más concretamente, en tres fuentes de prueba digital: los correos electrónicos, los WhatsApp, y las redes sociales. Con el objetivo central de analizar la valoración probatoria y las especificidades de aquellos, se ha querido partir de la insuficiente regulación legal hasta la reforma de 2015 y el cuestionamiento actual de la idoneidad de esta última. Entre ambas, el examen pormenorizado de la doctrina y jurisprudencia sobre las fuentes de prueba digital, que nos llevan a apreciar la necesidad de acomodar la legislación a las garantías constitucionales y europeas, afrontando paralelamente las dificultades que comportan unas técnicas digitales en constante evolución a la hora de adecuarse a las garantías probatorias.

## Palabras clave

investigación tecnológica, valor probatorio, nulidad, fuentes de prueba digital

## Tema

prueba tecnológica y proceso penal

\* Este trabajo ha sido realizado disfrutando del I+D (referencia DER2017-82146-P) y de la Ayuda para la mejora de la productividad científica de los grupos de investigación (MPC UdG 2016/002).

## Legal regulation and weighing up digital evidence (emails, WhatsApp, social networks): caught between insufficiency and uncertainty

### Abstract

This study focuses on technological media as a source of criminal procedural research, looking at three sources of digital evidence in particular: emails, WhatsApp and social networks. With the primary aim of analysing how the evidence is weighed up and the specific features of this technological media, the study is based on the insufficient legal regulation until the reform of 2015, and the current doubts as to whether or not the latter is suitable. The detailed exam of the doctrine and the precedent set for the sources of digital evidence lead us to consider the need to adjust the legislation to constitutional and European guarantees, simultaneously dealing with the difficulties of some constantly evolving digital techniques when it comes to complying with evidentiary guarantees.

### Keywords

technological investigation, evidentiary value, nullity, digital evidence sources

### Topic

technological evidence and criminal proceedings

## INTRODUCCIÓN: Consideraciones generales

El desarrollo de las comunicaciones ha generado una tremenda dependencia en el usuario que vierte una cantidad ingente de datos a través de internet en redes sociales, WhatsApp y otras aplicaciones de mensajería instantánea. Lo cierto es que la vida actual ofrece un número muy significativo de casos en que la tecnología es el medio utilizado para delinquir o la fuente básica para el desarrollo de la investigación.<sup>1</sup> Esta doble perspectiva abarca un sinfín de aspectos imposibles de abordar ahora: desde el amplio espectro de la «nueva criminalidad» que ofrecen estos medios,<sup>2</sup> hasta la utilización de recursos tecnológicos que

van aumentando conforme se escriben estas líneas.<sup>3</sup> Todos inciden en un campo sujeto a un difícil equilibrio: la mayor eficacia en la represión de los delitos, en general, pero también en ámbitos como el terrorismo, la criminalidad organizada o los delitos que implican a menores de edad; y paralelamente, el respeto y protección no solo de los derechos fundamentales, mediante instrumentos como la prueba ilícita, sino también en el conjunto de las garantías procesales incorporadas en el derecho a la presunción de inocencia y el derecho al debido proceso.<sup>4</sup>

Centrándonos en los medios tecnológicos como fuente esencial de muchas investigaciones, la ingente bibliografía sobre la prueba en la era digital, de internet como fuente

1. Las nuevas tecnologías en el enjuiciamiento penal ofrecen un doble enfoque: como objeto y como instrumento (Delgado Martín, 2016, capítulo, I, nota 5).
2. Asencio Mellado y Fernández López (2017).
3. Cabezudo Rodríguez (2016, pág. 9).
4. Desde el 11-S, el atentado en Londres y el 5-M, se incrementaron los instrumentos investigadores y represores, que los más recientes atentados yihadistas (París, Berlín, Niza, Barcelona) no han hecho sino afianzar, generando el consiguiente movimiento pendular entre la doble necesidad de que el Estado persiga los delitos y simultáneamente la protección de los derechos inherentes a la dignidad de las personas, cuya realización y preservación es el fundamento de la legitimación del poder y de la validez del derecho que crea (Armenta Deu, 2014, pág. 229-252; Delgado Martín, *op. cit.*, cap. II).

de prueba o de la prueba tecnológica,<sup>5</sup> eximen de analizar algunos aspectos, pero no de situar al lector en la realidad pasada y presente que se inicia mediante un brevísimo repaso de la situación normativa que ha corrido paralela a esta vorágine tecnológica.

## 2. La situación hasta 2015: carencias normativas e interpretación jurisprudencial

Hasta fechas relativamente recientes, la detención de la correspondencia privada, postal telegráfica y telemática que el procesado remitiera o recibiera y su apertura y examen se regía, por analogía, por el artículo 579 LECrim. Con tales mimbres se afrontó la legalidad de múltiples medidas adoptadas para investigar asuntos, en un contexto social complejo,<sup>6</sup> conscientes de la insuficiencia normativa e intentando soslayar entre otros efectos indeseados las condenas de tribunales nacionales e internacionales.

En cuanto a la protección de datos generados por el tratamiento de los dispositivos de almacenamiento masivo, la obsoleta regulación interna contenida en el Reglamento de aspectos accesorios a las actuaciones jurisdiccionales 1/2005, de 16 de septiembre y el artículo 230.5 LOPJ, que aseguraba el cumplimiento de la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, fue objeto de revisión por la publicación de diversas directivas europeas hasta la Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; modificada posteriormente por la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados

o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Ambas anuladas por las STJUE, de 8 de abril de 2014 (asunto Digital Rights) y de 21 de diciembre de 2016 (asunto Tele2 Sverige), poniendo de relieve la precariedad de las exigencias legales requeridas para conservar datos de carácter personal.<sup>7</sup>

Como se ha adelantado, la jurisprudencia nacional e internacional fue reiterando la necesidad de cambios legislativos a través de importantes resoluciones de las que se citan algunas de las más destacadas.

La STS de 19 de julio de 2001 denunció una vez más la insuficiencia del artículo 579 LECrim para sustentar las investigaciones a través de medios tecnológicos, concretamente la ausencia de previsión de supuestos que justifican la intervención, el objeto y el procedimiento de ejecución de la medida, así como la transcripción en acta del contenido de los soportes magnéticos, la custodia y destrucción de las cintas.

Posteriormente, la STC de 23 de octubre 2003 incidió en la falta de regulación sobre el plazo máximo de la duración de las intervenciones, por no existir prórrogas; resaltando, además, un aspecto significativo: que el artículo 579 LECrim solo habilita para limitar el secreto de las comunicaciones de las personas sospechosas, pero no de terceros con quienes aquellos se comunican. Particularmente rotunda fue la STC 145/2014, de 22 de septiembre, recordando, no obstante, que dicha insuficiencia no significa que el derecho vulnerara el artículo 8 CEDH, sino que correspondía al TC suplir las insuficiencias apreciadas en el precepto legal citado (sic 579) hasta que se produzca la necesaria intervención del legislador; función integradora que, sin embargo, en casos como el resuelto no alcanza a supues-

5. A título indicativo: Bueno de Mata (2017); Magro Servet (2006, pág. 107-115); Castillejo Manzanares (2010, pág. 11-43); Urbano Castrillo (2011); Delgado Martín (2017); Portal Manrubia (2013, pág. 19-41); Garrido Carrillo (2013-2014, pág. 553-590); Pinto Palacios y Puyol Capilla (2017); Vervaele (2012, pág. 27-86); Encinar del Pozo y Villegas García (2017).

6. La realidad española de escalada terrorista de principios de los ochenta lleva al Ejecutivo a abordar la regulación de las «observaciones telefónicas», dictando la LO 9/84 de 26 diciembre, contra la actuación de bandas armadas y elementos terroristas. Y como reacción contra la posible arbitrariedad en las medidas de vigilancia secretas ordenadas por las facultades discrecionales concedidas, surgió la tipificación en los artículos 192 bis y 497 bis CP, relativos a la colocación ilegal de escuchas telefónicas, introducidos por la LO 7/84 EDL1984/9281. En el ámbito procesal penal, sin embargo, no se acometió la reforma del obsoleto artículo 579 LECrim hasta la LO 4/1988 de 25 mayo 1988. Cfr. Gallego Sánchez (2010). Sobre la prueba ilícita, en esta tesis, Armenta Deu, (2014, *op. cit.*, pág. 235-237).

7. Gudín Rodríguez-Magariños (2017).

tos no contemplados en la norma, como la intervención de una conversación verbal entre personas detenidas a través del móvil.<sup>8</sup>

El TEDDHH, por su parte, en sentencia de 18 de febrero de 2003 (caso Prado Burgallo c. España) volvió a incidir sobre la ya denunciada carencia.<sup>9</sup>

En lo relativo a la protección de datos, las citadas resoluciones del TEJUE (casos Digital Rights y Tele2 Sverige)<sup>10</sup> pusieron de relieve que la regulación europea sobrepasaba los límites que exige el respeto al principio de proporcionalidad requeridos por los artículos 7, 8 y 52.1 de la CEDH de la Unión Europea, lo que condujo a declarar invalidada la Directiva 2006/24/CE.<sup>11</sup> Esta anulación no ha dejado de suscitar serias dudas sobre el efecto sobre la legislación española trasposición de aquella, ex Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.<sup>12</sup> El pasado 10 de noviembre, el Gobierno aprobó el proyecto de una nueva Ley orgánica de protección de datos.

### 3. La reforma de 2015

La LO 13/2015, de 5 de octubre, de modificación de la Ley de enjuiciamiento criminal, para el fortalecimiento de las

garantías procesales y la regulación de las medidas de investigación tecnológica, acometió la reclamada regulación, enfocando rectamente las medidas de investigación tecnológicas en muy diversos supuestos y estableciendo incluso unos «principios rectores» que recogían la jurisprudencia recaída durante años en torno a los presupuestos que deben concurrir para toda medida limitativa de derecho fundamental.<sup>13</sup>

Los medios de investigación tecnológica se centran en dos fuentes: los procesos comunicativos y los dispositivos y sistemas informáticos de almacenamiento de datos. Sobre los primeros recaerán eventualmente diversas medidas: a) la intervención de las comunicaciones sostenida a través de tecnologías de la información, y una modalidad de interceptación de comunicaciones personales efectuadas a través de servicios, como el correo electrónico, WhatsApp y similares o por redes sociales en general, y b) la propia red pública que sustenta estas comunicaciones. En lo referente a los dispositivos y sistemas informáticos y para obtener los datos que pueden alojar, cabe acudir al «acceso y registro para aprehender los datos relevantes contenidos en los mismos, y a la orden de entrega a los depositarios de esos datos», si se trata de información retenida en poder de terceros.<sup>14</sup>

Del conjunto de medidas posibles serán algunas de las contempladas en el apartado a) las que centren nuestra

- 
8. Tal era el caso resuelto en el que se otorgó el amparo solicitado por no respetarse que la medida de intervención fuera previsible para la persona afectada; no existiendo parámetros que marcaran el alcance de la discrecionalidad conferida a las autoridades competentes y la manera de su ejercicio, con la suficiente claridad como para proporcionar a las personas la protección adecuada contra una injerencia arbitraria. Se amparó a los condenados declarando ilícita la intervención telefónica del teléfono de la víctima que obraba en poder de los detenidos y que se realizó en dependencias policiales mientras estaban detenidos.
  9. Casos Fernández Saavedra c. España (2010) o Abdulkadir Coban c. España (2006), entre otros.
  10. STJUE, de 8 de abril de 2014 (asunto Digital Rights) y de 21 de diciembre de 2016 (asunto Tele2 Sverige).
  11. Las cuestiones que se estimaban a tal efecto eran la falta de determinación de las condiciones materiales y de procedimiento (pgf. 61), y la falta de información al usuario del hecho de la conservación de los datos (pgf. 39); la falta de la delimitación de los criterios objetivos de acceso y, concretamente, la falta de control jurisdiccional previo (pgf. 62); la falta de discriminación de los criterios temporales para la conservación de los datos, así como la falta de criterios objetivos en orden a garantizar que esta se limite a lo estrictamente necesario (pgf. 64); y la falta de garantía en orden a la seguridad y conservación de los datos, principalmente por la intervención de una autoridad independiente (pgf. 68) y la falta de control de los datos en caso de cesión de los mismos fuera del territorio de la Unión. Retengamos estos motivos para el examen posterior de la «cuestión prejudicial» planteada respecto a la regulación nacional contenida en la reforma de 2015, pendiente de resolución en el TJUE y a la que nos referiremos después.
  12. Rodríguez Lainz (2014, pág. 4). Sí suscita recelo el establecimiento de un plazo general de un año sin distinguir entre las diferentes clases de datos, algunos tan sensibles como la localización geográfica.
  13. Los artículos 579 a 588 integraron un nuevo capítulo III del título VIII del libro II que otorgó un nuevo y pormenorizado contenido a las «medidas de investigación tecnológicas». Una explicación pormenorizada del alcance y extensión de estos presupuestos que operan como «principios rectores» en Armenta Deu (2017, pág. 72-74, 183-185 y 195-200).
  14. Cabezudo Rodríguez (2016).

atención; concretamente las de interceptación encaminadas a captar el contenido de la comunicación intervenida junto con los datos de tráfico, que como elementos del proceso comunicativo gozan de la protección del derecho al secreto de las comunicaciones (art. 18.3 CE).<sup>15</sup> Cuestión distinta, y que no se abordará, será la observación, encaminada tan solo a determinar la procedencia e identidad de los interlocutores o alguno de esos datos de tráfico anexos al proceso comunicativo, medidas de registro de sistemas y dispositivos informáticos o de cesión de datos y archivos informáticos, entre otras.

#### 4. Valor probatorio de los correos electrónicos, mensajes de WhatsApp, Twitter, Instagram y otras redes sociales. Doctrina y jurisprudencia tras la reforma 2015

En la prueba electrónica cabe diferenciar dos modalidades: a) los datos o informaciones almacenados en un dispositivo electrónico (incluyendo sistemas informáticos y cualquier aparato informático o de tecnología digital, como los medios de almacenamiento masivo); y b) los que son transmitidos por cualquier red de comunicación abierta (internet, telefonía fija o móvil) o restringida, o a través de

una red de comunicación en la que no existe comunicación entre personas determinadas o determinables. Ante la imposibilidad de analizarlas de manera individualizada, centraré mi atención en las principales formas de fuentes de prueba digital por corresponder a aquellas que han suscitado mayor debate doctrinal y jurisprudencial.<sup>16</sup>

##### 4.1. Correo electrónico

Compuesto del contenido del mensaje junto a sus anexos (texto, imagen, vídeo) y de los datos de tráfico (fecha, hora, duración, origen y destino), una definición adecuada es la contenida en el artículo 2 h) de la Directiva 58/2002/CE, de 12 de julio.<sup>17</sup> La acreditación de un *mail* puede efectuarse mediante cualquiera de los dispositivos electrónicos de remisión o recepción, y/o en cualquiera de los servidores implicados, si bien la facilidad de acceso, según la empresa operadora tenga su sede o no en España y la eficacia probatoria de cada uno varía.<sup>18</sup> Con todo, resultará más sencillo probar el contenido del mensaje mediante el acceso a los dispositivos electrónicos utilizados para la comunicación por el emisor o el receptor del mail.

Teniendo presente que afectará al derecho fundamental a la intimidad y/o al secreto de las comunicaciones, según el acceso al correo electrónico tenga lugar con anterioridad a iniciar el proceso de comunicación o no sea así, y según se trate de los datos de cabecera o el contenido del mensaje,<sup>19</sup> la injerencia deberá:

15. Como es conocido, la medida de intervención puede recaer sobre: 1) el contenido del acto de comunicación; 2) los denominados datos de tráfico (origen de la comunicación, el destino, la ruta, el tiempo, la fecha, el tamaño, la duración del tipo de servicio, art. 1 del Convenio sobre Cibercrimen); 3) o la información personal del usuario o abonado que supuestamente efectúa la transmisión. Mediante tales medidas se reconoce sustantividad propia a la interceptación telefónica y telemática (Marchena Gómez y González-Cuellar Serrano, 2015, pág. 201).
16. Se sigue la opción de Delgado Martín (*op. cit.*, cap. 3).
17. Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que señala: «Todo mensaje de texto, voz o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que este acceda al mismo».
18. La conservación de los datos tendrá presente el cumplimiento de las obligaciones de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, si se trata de datos conservados por las entidades prestadoras de servicios; del artículo 588 ter j LECrim, cuando sean datos conservados por la operadora que no sean en cumplimiento de la ley citada anteriormente; del artículo 11.2 d) LO de protección de datos, cuando sean datos conservados por la compañía a iniciativa propia; o el caso contemplado en el artículo 588 ter LECrim.
19. No afecta al derecho a la comunicación, aunque sí al derecho a la intimidad, por ejemplo: el acceso a mensajes elaborados y aún enviados; la instalación de un software de control remoto en el dispositivo electrónico con el que se va a remitir el mensaje de *mail*; o de acceso al contenido de *mails* almacenados por la operadora. Sí afecta al derecho al secreto de las comunicaciones, en cambio, el acceso a un mensaje después de su envío por el remitente cuando está en proceso de transferencia hasta el destinatario, debiendo efectuarse conforme a las prescripciones del artículo 588 ter a y ss. LECrim; o cuando se trata de un *mail* que todavía no ha leído su destinatario y está almacenado por la operadora.

- cumplir los presupuestos de las medidas limitativas de derechos fundamentales;<sup>20</sup>
- aportarse al proceso mediante un medio probatorio adecuado: en formato papel, como documento electrónico;<sup>21</sup> y a través de copia del disco duro o del disco duro del servidor al que llegó el correo electrónico, con su correspondiente *código hash* calculado ante fedatario público;<sup>22</sup> acompañándose del correspondiente informe, cuyas conclusiones podrán incorporarse mediante prueba pericial;<sup>23</sup> o recurriendo a algún «prestador de servicio de confianza», conforme a lo dispuesto en el Reglamento UE/910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior;<sup>24</sup>
- salvaguardar la cadena de custodia (arts. 777.2,1,II y III LECrim), y
- reproducirse correctamente en el juicio (art. 797,2,1,II y III LECrim).

Cuestión diferente será la valoración que corresponda a cada uno de los medios probatorios y la eventual valoración conjunta, aplicando las reglas de la sana crítica, o lo que es igual, el principio de libre valoración (art. 741 LECrim) y el resultado final. Aspectos que dependen, a su vez, del medio probatorio incorporado al proceso, su autenticidad

y la postura procesal de las partes. Así, por ejemplo, la utilización como prueba del documento electrónico, a falta de norma específica en la Ley de enjuiciamiento criminal, se adecuará a lo dispuesto en el artículo 230.1 LOPJ, Ley 59/2003, artículo 3 de la Firma electrónica, y artículo 299.2 LEC, por analogía, conforme a lo dispuesto en el artículo 4 LEC;<sup>25</sup> en tanto a la prueba electrónica de documentos públicos y de documentos oficiales corresponde, también por analogía, la valoración establecida en el artículo 319.1 y 2 LEC, ya que los documentos electrónicos privados deben pasar el filtro de la autenticidad e integridad de los datos a través de la llamada «copia forense».<sup>26</sup>

La impugnación de la autenticidad o integridad por alguna de las partes revertirá en la necesidad de acreditar los hechos mediante otro medio probatorio, que atendidas las complejidades técnicas suele ser la pericia,<sup>27</sup> aunque no solo.<sup>28</sup>

#### 4.2. WhatsApp y otros sistemas de mensajería instantánea

Las especiales características de esta forma de comunicación entre usuarios mediante una aplicación para teléfonos móviles y *smartphones* que permite enviar mensajes de texto, notas de audio y vídeo, compartir contactos o la propia ubicación presentan algunas diferencias con el correo electrónico y SMS, ya que la información transmi-

- 
- Artículo 588 bis a) a artículo 588 bis k LECrim. STS 877/2014, de 22 de diciembre.
  - Previa clonación del disco duro ante LAJ o notario, elaborando posteriormente un informe de experto que podrá presentarse en el proceso mediante el correspondiente peritaje. Rubio Alamillo (2016). STS 298/2015, de 13 mayo.
  - Pereira Puigvert (2013); Bueno de Mata (2016a, pág. 248 y ss).
  - El informe pericial informático (de técnicos especialistas) sirve para afianzar el valor probatorio de un correo electrónico mediante el análisis del equipo o equipos que lo contiene, los datos de cabecera y sobre todo su correspondencia cronológica. Martínez Carvajal Hedrich (2013).
  - Reglamento (UE) núm. 910/2014, del Parlamento Europeo.
  - A los «pantallazos» obtenidos del teléfono móvil se les niega valor de documento, entendiéndose que se trata de una prueba personal documentada posteriormente para su incorporación a la causa (STS 300/2015, de 19 de mayo; negativa que ya se predicaba de las transcripciones de diálogos o conversaciones mantenidas por teléfono (SSTS 1024/2007, 1157/2000 o 942/2000). Negativa que se extiende a los pantallazos de Facebook (STS 782/2016, de 16 de octubre).
  - Captura de todos los datos de la fuente de evidencia electrónica para que permanezca inalterada; e informe pericial por unidades policiales especializadas o peritos informáticos no públicos. El código *hash* es el principal instrumento técnico al efecto. Delgado (*op. cit.*, cap. I, pág. 14), y Pereira Puigvert, *op. cit.*
  - Sobre la relevancia de la pericia en este ámbito, Rodríguez Lainz (2015, *op. cit.*, y nota 52).
  - En el caso resuelto por la STS 300/2015, de 19 de mayo, se aprecia la autenticidad de un diálogo mantenido a través de Tuenti entre la víctima de abusos sexuales y un amigo al que relata varios incidentes, y que constituye prueba suficiente de cargo, por dos razones: que la propia víctima fue quien puso a disposición del juez su contraseña de Tuenti por si esta era puesta en duda, como ocurrió; y que el interlocutor fuera propuesto como testigo acudiendo al plenario y pudiendo ser interrogado por las acusaciones y la defensa, corroborando que tal conversación se mantuvo. Un juicio crítico en De Bueno Mata (2016b).



tida no se conserva por un servidor externo, se utilizan protocolos de seguridad para garantizar el cifrado de la información<sup>29</sup> y resulta disponible en multiplataforma: IOS, Android, Windows Phone. El hecho de que el contenido no quede almacenado en el servidor del administrador impide que la autoridad judicial pueda solicitar a la empresa prestadora del servicio que certifique el contenido de mensajes enviados o recibidos, teniendo que acudir a los dispositivos electrónicos usados para su conversación.<sup>30</sup> Cuestión diferente será la de los datos de tráfico generados durante la conservación de WhatsApp y que no constituyen contenido de la conversación (origen y destino, ruta, hora, tamaño y duración de la comunicación).<sup>31</sup>

Como en los restantes medios analizados, el enorme riesgo de manipulación o de generación de mensajería instantánea, suplantación de origen o de identidad<sup>32</sup> condujo a diversos pronunciamientos que recalaban la importancia del medio de aportación al proceso y del análisis pericial de los datos examinados respecto de comunicaciones cuya realidad o autenticidad se cuestiona,<sup>33</sup> así como a la necesidad del análisis detenido de los correspondientes terminales, si es posible entre supuestos emisor y receptor, así como que no haya sido manipulado.<sup>34</sup>

A lo largo de varias resoluciones se estableció una «regla de carga probatoria» que desplazaba a quien aportara o a quien pretende valerse de su valor probatorio acreditar el verdadero origen de la comunicación, identidad de los interlocutores y la integridad de su contenido.<sup>35</sup> Con todo, el rigor de este desplazamiento de la carga probatoria se fue

matizando notablemente, de manera que si bien resulta taxativa respecto de los llamados «pantallazos» o simples impresiones de concretas comunicaciones o de su rastro,<sup>36</sup> en cuanto al resto –aportación mediante soportes electrónicos originales o copia, o acompañando el original– se apela a un examen singularizado y cauteloso.<sup>37</sup>

Si quisiéramos elaborar una sucesión esquemática de los pasos a seguir en la valoración, transcurriría así:

- la aportación del original otorga mayor facilidad probatoria a cualquier copia o «pantallazo», al igual que la falta de impugnación puede ser valorada como aceptación tácita de su autenticidad y validez;
- cuando se impugne la autenticidad, corresponde a quien la ha aportado reforzar aquella, lo que generalmente se llevará a cabo mediante la prueba pericial. Pericia que, por su parte, siendo como es un medio probatorio idóneo por las especificidades técnicas que concurren, no constituye, empero, un medio incontestable, ya que puede depender a su vez de circunstancias ajenas a la propia pericia y del buen quehacer del mismo perito o incluso de la concreta pericia del caso.<sup>38</sup>

Ahora bien, ni la simple impugnación desvirtuará el valor probatorio, en todo caso, ni su resultado tendrán un efecto determinante. La valoración, como es conocido, la lleva a cabo el juez con arreglo a las reglas de la sana crítica, contrastando todos los medios probatorios, lícitos, admitidos y practicados conforme a las garantías probatorias,<sup>39</sup> de

29. Rodríguez Lainz (2015); Arrabal Platero (2017).

30. García Mescua (2018).

31. Dicha información, útil eventualmente para el proceso penal, podrá ser reclamada si se conserva por la operadora.

32. Una amplia y pormenorizada descripción de los posibles métodos y niveles de intrusión, así como de las eventuales técnicas forenses de detección del fraude en el trabajo de Rodríguez Lainz (2015) y en De Bueno Mata, *op. cit.*

33. STS 342/2013, de 17 de abril y notas 30 y 52.

34. La investigación se centrará en la memoria interna del terminal, volcar la presencia de códigos propios de esos terminales, dirección IP del servidor que reenvía los datos, en su caso y otros aspectos que figuran en las tarjetas de memoria SD (Delgado Martín, 2016, *op. cit.*, cap. 3).

35. STS 300/2015, de 19 de mayo.

36. Representaciones en papel impreso de copias de pantalla o pretendidas comunicaciones emitidas y/o recibidas por quien las aporta o por alguien que las ha facilitado a las que se niega valor probatorio *per se*. Sentencias citadas en nota 26.

37. STS 300/2015, de 19 mayo; 298/2015, 13 de mayo; y 786/2015, 4 de diciembre.

38. Así por ejemplo, que pueda acceder a la fuente original o no sea así; que se pueda cotejar la realidad de la existencia de la comunicación, su recepción y la coincidencia de las versiones. Sin rechazar que pueda variar la misma calidad de los conocimientos y medios empleados por el perito. *Cfr.* Rodríguez Lainz (2003, pág. 391-396).

39. En el caso de ilicitud probatoria, cabe haber excluido la fuente probatoria, pero también es posible que sea el momento de la valoración cuando el juez tiene todos los elementos para discernir sobre la concurrencia de infracciones al derecho fundamental que determinen que no puede ser objeto de valoración (Armenta Deu, 2011, pág. 141-143).

forma que tanto la valoración conjunta con otros medios probatorios puede conducir a que la pretendida falta de autenticidad quede contradicha por otros medios, como que se ratifique el contenido por parte de los interlocutores o el testimonio de la testigo denunciante,<sup>40</sup> que se facilite el acceso a la fuente original<sup>41</sup> o que se susciten contradicciones entre lo declarado por el acusado.<sup>42</sup>

### 4.3 Redes sociales y otros elementos web

Del inabarcable mundo de las redes sociales<sup>43</sup> me centraré en el hecho de que cada usuario construya un perfil público o semipúblico en un sistema delimitado o cerrado y en que se elabora una lista de otros usuarios que comparten relaciones, pudiendo recorrerse la lista de relaciones que las personas tienen con otras del sistema.<sup>44</sup>

Entre las múltiples consecuencias jurídicas que implica este quehacer, presenta relevancia probatoria la información obtenida de las redes sociales y la prueba de los hechos delictivos cometidos en las mismas.<sup>45</sup> En el primer sentido, la investigación de los hechos requerirá fuentes y medios clásicos y novedosos orientados a investigar la huella digital, la autoría y/o la localización de la empresa prestadora del servicio. Por lo que hace a la información obtenida en las redes sociales, se orientará a analizar el rastro digital, tanto para investigar un ilícito cometido en la

red como fuera de ellas. La titularidad de la cuenta puede ser también el objeto de investigación, lo que se hará averiguando la dirección IP utilizada para colgar el contenido ilícito y, a partir de ahí, la cesión de datos de identificación y localización del dispositivo, identificación que precisará de autorización judicial (art. 588 ter k LECrim).<sup>46</sup>

A falta de un precepto que regule la aportación de fuentes de prueba de estas características,<sup>47</sup> cabrá que el Ministerio Fiscal o las partes proporcionen información contenida en las redes sociales, tanto de perfiles propios como ajenos a cuyo contenido se pueda acceder lícitamente, así, la información insertada voluntariamente en la red para ser compartida con otros usuarios no goza de la protección del secreto de las comunicaciones; sin embargo, la amplitud de actividades obligará a un examen más concreto, en supuestos como la información transmitida entre un grupo limitado o identificado de interlocutores, ámbito en el que sí resultaría aplicable el artículo 18.3 CE. Otro medio de aportación es a través de la información almacenada en un servidor, aspecto este que cuando -como es frecuente- se trata de servidores que tienen su sede fuera del territorio español, genera no pocos problemas cuya eventual solución discurre a través de la cooperación judicial internacional,<sup>48</sup> ya sea mediante la aplicación del Convenio de Budapest, para países fuera de la UE,<sup>49</sup> y en el marco comunitario, el Convenio de 29 de mayo, de

40. Sentencia 702/2015, de 24 de noviembre, de la Sección 27.ª de la AP de MD.

41. La simple aceptación o no impugnación propició su valoración probatoria en SSTS 899/2014, de 26 de diciembre (WhatsApp entre víctima de malos tratos y un amigo en donde narra la situación); 126/2015, de 12 de mayo; 258/2015, de 8 de mayo (conversaciones a través de chats con un menor de edad para proponerle relaciones sexuales); 264/2015, de 7 de mayo; 298/2015, de 13 de mayo; o 515/2013, de 13 junio.

42. Así por ejemplo, en un caso en que se pretendía la valoración de un hecho como incontestable de un «pantallazo» de Facebook en donde la menor se aumentaba la edad, la Sala valoró la contradicción sobre ese dato, ante el juez de instrucción, donde admitió conocer la edad de la víctima, y el plenario cuando lo negó (STS 782/2016, de 15 de octubre).

43. Información generada en las web horizontal (con carácter generalista) y vertical (dirigida a usuarios con perfil específico y predefinido); redes de difusión de conocimiento (aquellas en cuyos servicios a través de internet cuenta con personas con intereses comunes que interactúan en igualdad de condiciones); o redes sociales: directas, que suelen carecer de usuarios con perfil visible para todos, existiendo alguien que controla y dirige las discusiones en un tema concreto (foros, blogs, etc.) (Davara Fernández de Marcos, 2015, *passim*).

44. Agustino Guilayn y Monclús Ruiz (2016).

45. Se sigue en esta exposición el orden de Delgado Martín (*op. cit.*, cap. 3).

46. Sobre los pantallazos, como instrumento habitual de incorporar el texto del correo electrónico, destacan su escaso valor *per se*, y la necesidad de acompañarlos del correspondiente informe pericial, para demostrar la autenticidad de las conversaciones, así como del uso de la red social Tuenti, STS 300/2015, de 19 de mayo, 281/2016, de 14 de septiembre, así como las resoluciones que figuran en la nota 28. También: Rodríguez Lainz (2015, *op. cit.*)

47. La única excepción, y con el carácter específico que le otorga su ámbito de aplicación, es el artículo 11 b) Ley 4/2015 de 27 de abril, del estatuto de la víctima del delito.

48. Art. 276 LOPJ.

49. Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, ratificado por España en 2010 (BOE de 17 de septiembre de 2010) y aplicable para cualquier proceso penal en orden a obtener pruebas electrónicas de los delitos (art. 23).

asistencia judicial en materia penal entre los miembros de la Unión Europea, la Directiva 2014/41/CE, Orden Europea de Investigación penal,<sup>50</sup> y en aquello no comprendido por la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE.

En lo relativo a la valoración probatoria, cabe recordar lo hasta ahora expuesto en un doble plano: 1.º) que las distintas informaciones insertas en el perfil abierto son colgadas libremente, por lo que difícilmente afectarán al derecho a la intimidad; y 2.º) que en caso de limitar algún derecho fundamental, como el sitio web de acceso restringido a un grupo cerrado de personas, la valoración del medio probatorio aportado (documento, inspección ocular, pericia, testimonio o interrogatorio de parte o del acusado) debería superar un doble control: que la fuente ha sido obtenida salvaguardando rigurosamente los requisitos contemplados en los artículos 588 bis LECrim (con carácter general) y lo dispuesto en el artículo 588 ter LECrim, en particular, así como que ha sido incorporada al proceso y en su caso reproducidas en el juicio oral con las debidas garantías de audiencia y contradicción.<sup>51</sup> De otra forma, la ilicitud probatoria, si no provocó su exclusión por no resultar lo más procedente,<sup>52</sup> no podría enervar la presunción de inocencia; efecto similar al que se ocasionaría, aun no tratándose de una fuente de prueba ilícitamente obtenida, en el caso de cualquier medio de prueba que no cumpla con los requisitos comprendidos en el derecho a utilizar todos los medios pertinentes para la defensa y a la presunción de inocencia.<sup>53</sup>

## 5. La incertidumbre tras la cuestión de prejudicialidad (Asunto C-207/16)

En este contexto, y mediante auto de la AP de Tarragona, el 14 de abril de 2016, se instó una «cuestión prejudicial ante el TSJUE» solicitando un pronunciamiento sobre los artículos 579 y 588bis LECrim -donde se definen los presupuestos que autorizan la injerencia del Estado en las comunicaciones telemáticas de los sospechosos- por si pudieran ser contrarios a los principios y derechos de la Unión (arts. 7 y 8 CDFUE y 8 CEDH).<sup>54</sup> Se destaca, en apretada síntesis, que la injerencia de intensa lesión para los derechos fundamentales afectados se efectúa mediante una fórmula que define el umbral penológico de manera tal que no satisfacen la exigencia de proporcionalidad requerida por el derecho de la Unión Europea, especialmente en cuanto a la delimitación del estándar de gravedad que justifica dicha injerencia. En otros términos, se cuestiona el criterio de «gravedad suficiente» identificado únicamente por la pena que pueda imponerse al delito que se investiga, sin concretar en la conducta particular nivel de lesividad para bienes jurídicos individuales o colectivos; y asimismo, en caso de que sí se ajustara, se pregunta cuál debería ser el nivel mínimo de la pena imponible, cuestionando si este es compatible con una previsión general de límite de tres años de prisión, como se contempla en los artículos 579 y 588 bis, ambos de la LECrim. Fuente confesada de este planteamiento es la STJUE de 8 de abril de 2014, a cuyos fundamentos 46 a 48, 52, y 53 y siguientes nos remitimos<sup>55</sup> en espera de la resolución a la citada Cuestión.<sup>56</sup>

- 
50. Cuyo artículo 3 extiende la posibilidad de emitir una OEI a todos los medios de prueba, excepto la creación de un «equipo conjunto de investigación», extendiéndose incluso a medios diferentes a los de la OEI en los supuestos del artículo 10, a excepción de la identificación de personas que sean titulares de un número de teléfono o una dirección IP determinados, en cuyo supuesto se requiere que tal medida esté contemplada en el Estado de ejecución (art. 10, 2, e).
51. Recuérdese aquí lo expuesto respecto al modo de incorporación al proceso y la relevancia de la prueba pericial técnica, es decir, la efectuada por un perito cualificado en aspectos informáticos. Al respecto, Sáez-Santurtún Prieto (2105) y Martínez Carvajal Hedrich (2013).
52. Sobre el momento de apreciación: STS 255/2017, de 6 de marzo y 85/2017, de 15 de febrero.
53. Nota 40, y en particular, Sáez-Santurtún Prieto (2015).
54. Accesible en <<http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62016CN0207&from=ES>>.
55. Vid. nota 12. Adviértanse las similitudes en cuanto a discriminación de criterios temporales o falta de criterios objetivos para garantizar una limitación estrictamente necesaria, por ejemplo.
56. Enviado el trabajo y en periodo de revisión se han publicado las «Conclusiones del Abogado General» (3 de mayo de 2018). Atendiendo a que, pese a su relevancia y a que suelen ser ciertamente un adelanto del sentido del fallo posterior, la limitación de la extensión del trabajo, de un lado, y sobre todo, de otro, la prudencia, aconsejan dejar para un posterior comentario no solo dichas Conclusiones, sino el fallo final, que al fin y al cabo depende del criterio de los magistrados.

## 6. Reflexión final

Las medidas tecnológicas utilizadas a la hora de obtener la fuente de prueba digital pueden resultar muy invasivas, generando importantes riesgos de vulneración de derechos fundamentales; en este ámbito se abre un importante interrogante en función de la resolución que obtenga la cuestión prejudicial pendiente de resolución por el TJUE. Paralelamente, por su complejidad y volatilidad, requieren adecuar la regulación de la prueba en sus diferentes fases: obtención, incorporación al proceso y valoración; aspecto conexo con el anterior y que obliga a un nuevo esfuerzo legislativo que dé respuesta a las deficiencias señaladas en este y otros análisis.

Con todo, y sin restar importancia al tema central de este trabajo, las complejidades de la prueba digital no pueden empañar que, a la postre, la valoración probatoria se proyectará en primer lugar sobre la calificación de la validez y licitud de la fuente correspondiente, y en segundo lugar, sobre la ponderación de la eficacia o fuerza convincente del conjunto de medios, según las reglas de la sana crítica; de manera que solo la garantía de ambos extremos enerva válidamente la presunción de inocencia.<sup>57</sup> Las seis vertientes: condenar con suficientes pruebas de cargo; con base en pruebas lícitas; motivando la convicción probatoria; sobre la base de pruebas suficientes; o sobre la base de una motivación lógica, irregular o concluyente, aunque no conformen compartimentos estancos, deben ser respetadas para alcanzar una condena como contenido primario del autónomo derecho a un proceso con todas las garantías (art. 24.2 CE).<sup>58</sup>

### Bibliografía citada o recomendada

- AA. VV. (2017). *Justicia Penal y nuevas formas de delincuencia*, J. M. ASECIO MELLADO(dir.). M. FERNÁNDEZ LÓPEZ (coord.). Tirant lo Blanch.
- AA. VV. (2017). *Fodertics 6.0 7) Los nuevos retos del derecho ante la era digital*-. F. BUENO DE MATA (dir.). Comares.
- AGUSTINOY GUILAYN, A.; MONCLÚS RUIZ, J., (2016). «Aspectos legales de las redes sociales». Bosch.
- ARMENTA DEU, T. (2017). «Lecciones de derecho procesal». 10ª edición, Marcial Pons.
- ARMENTA DEU, T. (2014). «Limitación de derechos fundamentales y prueba ilícita» En: *Estudios de Justicia Penal*. Marcial Pons.
- ARMENTA DEU, T (2011). «La prueba ilícita. Un estudio comparado». 2ª ed., Marcial Pons.
- ASECIO MELLADO, J. M.; FERNÁNDEZ LOPEZ (2017). «Justicia penal y nuevas formas de delincuencia». Ed. de la Universidad de Alicante.
- ARRABAL PLATERO, P. (2017). «El WhatsApp como fuente de prueba». En: O. FUERTES (coord.). *El proceso penal: cuestiones fundamentales*. Valencia: Tirant lo Blanch.
- BUENO DE MATA, F. (2016a). «Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de WhatsApp, Snapchat o Telegram». En: AA. VV., «Hacia una justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e informática». Salamanca: Ratio Legis.
- BUENO DE MATA, F. (2016b). «La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica». *Diario la Ley*, nº 8728, 23 de marzo.

57. STC 33/2002; STS 653/2016, de 18 de julio, F.J. n.º 21 y antes: STS 255/2017, de 6 de marzo, F. J. n.º 7. SSTC 109/1986, 68/1988 y, entre otras muchas, 207/2007 y 145/2014.

58. STS 255/2017, de 6 de marzo, F.J. n.º 8 y STS 675/ 2015, de 10 de noviembre y 250/2017, F.J, n.º 6.

- BUENO DE MATA, F. (2016c). «La validez de los “screenshots o “pantallazos” como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo». En: A. M. NEIRA PENA (dir.), BUENO MATA y J. PEREZ GIL (coord.). «Los desafíos de la justicia en la era post crisis». Atelier.
- CABEZUDO RODRÍGUEZ, N. (2016). «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal». *BMJ*, año LXX, número 2186, febrero.
- CASTILLEJO MANZANARES, R. (2010). «La prueba en el proceso penal: el documento electrónico». *Revista de Derecho Penal*, n.º 29.
- DAVARA FERNÁNDEZ DE MARCOS, L. (2015). «Implicaciones Socio-Jurídicas de las Redes Sociales». Thomson Reuters Aranzadi.
- DELGADO MARTÍN, J. (2016). «Investigación tecnológica y prueba digital en todas las jurisdicciones». *La Ley*, ed. digital.
- DELGADO MARTÍN, J. (2017). «La prueba electrónica en el proceso penal». *Diario La Ley*, n.º 8167.
- ENCINAR DEL POZO, M. A.; VILLEGAS GARCÍA (2017). «Validez de medios de prueba tecnológicos». *Diario la Ley*, n.º 9005, 21 de junio.
- FUENTES SORIANO, O. (2017). «Comunicaciones telemáticas: práctica y valoración de la prueba». AA. VV. *El proceso penal: cuestiones fundamentales*. Tirant lo Blanch.
- GALLEGO SÁNCHEZ, G. (2010). «Sobre el secreto de las comunicaciones, el art. 579 LECrim y las intervenciones telefónicas». *El Derecho. com*, <[http://www.elderecho.com/tribuna/penal/secreto-comunicaciones-LECrIm-intervenciones-telefonicas\\_11\\_159055012.html](http://www.elderecho.com/tribuna/penal/secreto-comunicaciones-LECrIm-intervenciones-telefonicas_11_159055012.html)>
- GARCÍA MESCUA, D. (2018). *Aportación de mensajes de WhatsApp a los procesos judiciales. Tratamiento procesal*. Comares.
- GARRIDO CARRILLO, F. J. (2013-2014). «La prueba electrónica en los procesos civiles y penales». *Revista de la Facultad de Derecho de la Universidad de Granada*, n.º 16-17.
- GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E. (2017). «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, n.º 125.
- MAGRO SERVET, V. (2006). «La prueba pericial informática. La utilización de los medios de prueba informáticos en el proceso penal». *La Ley Penal*, n.º 33.
- MARCHENA GÓMEZ, M.; GONZÁLEZ-CUÉLLAR SERRANO, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal en 2015*. Castillo de Luna, Ediciones Jurídicas.
- MARTÍNEZ CARVAJAL HEDRICH, E. (2013). «Valor probatorio de un correo electrónico». *Diario La Ley*, n.º 8014, febrero.
- PINTO PALACIOS, F.; PUYOL CAPILLA, P. (2017). «La prueba en la era digital». *La Ley*. Wolters Kluwer.
- PEREIRA PUIGVERT, S. (2013). *La exhibición de documentos y soportes informáticos en el proceso civil*. Thomson Reuters-Aranzadi.
- PORTAL MANRUBIA, J. (2013). «La regulación de la prueba electrónica en el proceso penal». *Revista de Derecho y Proceso Penal*, n.º 31.
- RODRÍGUEZ LAINZ, J. L. (2015). «Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2ª, 300/2015, de 19 de mayo)». *Diario la Ley*, n.º 8569, sección doctrina, 25 de junio de 2015.
- RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la Ley española sobre conservación de datos relativos a las comunicaciones». *La Ley*, n.º 8308.



- RODRÍGUEZ LAINZ, J. L. (2003). *Intervención judicial en los datos de tráfico de telecomunicaciones electrónicas*. Bosch.
- RUBIO ALAMILLO, J. (2016). «El correo electrónico como prueba en procedimientos judiciales». *Diario la Ley*, n.º 8808, Sección Práctica Forense 21 de julio de 2016.
- SÁEZ-SANTURTÚN PRIETO (2105). «La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 de mayo de 2015». *Diario la Ley*, n.º 8637.
- URBANO CASTRILLO, E. (2011). «La regulación legal de la prueba electrónica: una necesidad pendiente». *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*. n.º 82.
- VERVAELE, J., (2012). «Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal». En: «El proceso penal en la sociedad de la información». *La Ley*.

### Cita recomendada

ARMENTA DEU, Teresa (2018). «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, whatsapp, redes sociales): entre la insuficiencia y la incertidumbre». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 67-78. UOC [Fecha de consulta: dd/mm/aa]  
 <<http://dx.doi.org/10.7238/idp.v0i27.3149>>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre la autora

Teresa Armenta Deu  
 teresa.armenta@udg.edu

Catedrática de Derecho Procesal  
 Universitat de Girona

<http://www2.udg.edu/professorat/Planapersonal/tabid/8656/ID/51892/language/es-ES/Default.aspx>

Facultat de Dret  
 Campus Montilivi  
 17003 - GIRONA  
 Despatx: 219

